

الحماية الجنائية للأمن الإلكتروني

دكتور

حازم حسن الجمل

دكتوراه في الحقوق - جامعة المنصورة

دار الفكر والقانون

١ شارع الجلاء - أمام بوابة الجامعة

المنصورة - برج آية

تليفون: ٢٢٣٦٢٨١ / ٥٠ / محمول: ٠١٠٠٦٠٥٧٧٦٨

الحماية الجنائية للأمن الإلكتروني

دكتور

حازم حسن الجمل

دكتوراه في الحقوق

جامعة المنصورة

2015

دار الفكر والقانون

للنشر والتوزيع

1 ش الجلاء أمام بوابة الجامعة برج آية

تليفكس : 0020502235671 تليفون : 0502236281

محمول 00201006057768

اسم الكتاب : الحماية الجنائية للأمن الإلكتروني

اسم المؤلف: دكتور/ حازم حسن الجمل

الطبعة الأولى

سنة الطبع : 2015

رقم الإيداع بدار الكتب المصرية : 26823

الترقيم الدولي: 9789777170438

الناشر : دار الفكر والقانون للنشر والتوزيع

1 ش الجلاء أمام بوابة الجامعة برج آية

تليفكس : 0020502235671 تليفون : 0502236281

محمول 00201006057768

dar.elfker@hotmail.com

المحامي / أحمد محمد أحمد سيد أحمد

إهداء

إلى فقراء هذا العالم ...

إلى روح والدي الساكنة في الأبدية... إلى أسرتي... إلى ابنتي هايدي وندي،

فلذتا كبدي وقُرتا عيني ..

د. حازم حسن الجمل

شكر وتقدير وعرفان

في البداية نشكر المولى عز وجل على عظيم نعمه علينا، وتوفيقه لنا في إتمام هذه الدراسة. ثم أتوجه بخالص الشكر والتقدير والعرفان بأسمى معاني الحب والامتنان والثناء إلى أستاذي الفاضل العالم الجليل العميد أ.د / أحمد شوقي عمر أبو خطوه (أستاذ القانون الجنائي بكلية الحقوق، جامعة المنصورة، وعميد الكلية الأسبق)

د. حازم حسن الجمل

مقدمة

أولاً : موضوع الدراسة :

يتعلق موضوع هذه الدراسة بالحماية الجنائية (الموضوعية والإجرائية) للأمن الإلكتروني في التشريع الإماراتي، حيث أصبح الاعتداء على الأمن الإلكتروني من أخطر الظواهر المستحدثة تأثيراً على أمن الدولة، وعقيدتها، واقتصادها، وتراثها الحضاري، والنظام العام فيها، والسلم الاجتماعي، وكذلك العلاقات الدولية والإقليمية⁽¹⁾.

ثانياً : أهمية الدراسة :

تكتسب هذه الدراسة أهميتها من خلال البحث عن مدى قصور قواعد الحماية الجنائية (الموضوعية والإجرائية) المقررة بموجب المنظومة التشريعية، التي تستهدف بها المشرع الإماراتي حماية الأمن الإلكتروني، باعتبارها مدخلاً هاماً لمصالح أساسية وهامة تشمل أمن الدولة، واقتصادها، وعلاقاتها بين الدول...الخ.

(1) أنظر : المادة (14) من مرسوم بقانون اتحادي رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني، في دولة الإمارات العربية المتحدة، الصادر بتاريخ 2012/8/13م، الجريدة الرسمية رقم (540)، ص 13.

ثالثاً : مشكلات الدراسة :

تعالج هذه الدراسة كثير من المشكلات ذات الصلة بسياسة ومنهج وخطة المشرع الإماراتي بشأن تجريم، وملاحقة الاعتداء على الأمن الإلكتروني. وما كشف عنه بالضرورة الواقع العملي من قصور في بعض الأحيان، أو عدم التوائم والتناسق التشريعي بين مصادر الحماية الجنائية المختلفة في أحيان أخرى.

رابعاً : أهداف الدراسة :

تهدف هذه الدراسة إلى التعرف على جرائم الاعتداء على الأمن الإلكتروني، وخطورتها، وانعكاساتها المختلفة، وكذلك استكشاف أوجه قصور قواعد الحماية الجنائية المقرر في هذا المجال الحيوي، بهدف التوصل إلى رسم معالم النموذج التشريعي الأمثل للمصالح محل الحماية الجنائية.

خامساً : خطة الدراسة :

في سبيل إلى بيان الأهداف المنشودة من هذا البحث، فإن دراستي لهذا الموضوع ستكون على نحو الخطة التالية :

الفصل الأول : التعريف بجرائم الاعتداء على الأمن الإلكتروني.

الفصل الثاني : الحماية الجنائية الموضوعية للأمن الإلكتروني.

الفصل الثالث : الحماية الجنائية الإجرائية للأمن الإلكتروني.

الفصل الأول

التعريف بجرائم الاعتداء على الأمن الإلكتروني

في سبيل التعريف بجرائم الاعتداء على الأمن الإلكتروني، يقتضى الأمر أن نبحث في مفهوم الأمن الإلكتروني، ومصادر حمايته القانونية، ثم نخرج بعدها إلى تحديد المصالح محل الحماية الجنائية وسبلها.

المبحث الأول : مفهوم الأمن الإلكتروني ومصادر الحماية الجنائية.

المبحث الثانى : تحديد المصالح محل الحماية الجنائية وسبلها.

المبحث الأول

مفهوم الأمن الإلكتروني ومصادر الحماية الجنائية

أولاً : مفهوم الأمن الإلكتروني :

يقصد بالأمن الإلكتروني (تأمين وحماية) الشبكة المعلوماتية، وشبكة الاتصالات، ونظم المعلومات، وعمليات جمع المعلومات، باستخدام أي من الوسائل الإلكترونية⁽¹⁾.

ثانياً : مصادر حماية الأمن الإلكتروني في التشريع الإماراتي :

تعتبر القوانين، والمراسيم التالية، من أهم مصادر الحماية التشريعية للأمن الإلكتروني في دولة الإمارات العربية المتحدة⁽²⁾ : -

- المرسوم بقانون اتحادي رقم (3) لسنة 2012م، بشأن إنشاء الهيئة الوطنية للأمن الإلكتروني⁽³⁾. وقد نص المشرع الإماراتي بموجب المادة

(1) المادة الأولى من مرسوم بقانون اتحادي رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني.

(2) ينظم الحماية الجنائية للبيئة المعلوماتية في الولايات المتحدة الأمريكية التشريع الفيدرالي الصادر سنة 1984 المعدل في السنوات التالية (1986، 1990، 1994، 1996، 2001). وفي فرنسا صدر أول تشريع سنة 1979 لحماية الحريات والمعطيات، وفي سنة 2004 صدر قانون يتعلق بالاقتصاد الرقمي.

(3) صدر بتاريخ 2012/8/13م الموافق 25 رمضان 1433هـ ونشر في الجريدة الرسمية رقم (540)، ص 13.

رقم (23) من هذا المرسوم على إلغاء كل حكم يخالف أو يتعارض مع أحكام هذا المرسوم بقانون.

- المرسوم بقانون اتحادى رقم (5) لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات⁽¹⁾، وقد ألغى المشرع الإماراتى بموجب المادة رقم (50) من هذا المرسوم القانون الاتحادى رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات، وكذلك نص صراحة بموجب هذه المادة على إلغاء كل حكم يخالف أو يتعارض مع أحكام هذا المرسوم بقانون.

- القانون الاتحادى رقم (1) لسنة 2006م، في شأن المعاملات والتجارة الالكترونية⁽²⁾.

والجدير بالملاحظة أنه رغم التكامل بين المصادر القانونية السالفة البيان في تقرير الحماية للأمن الالكترونى، إلا أن النص صراحة بموجب هذه القوانين على إلغاء كل حكم يخالف أو يتعارض مع أحكامها، ربما يثير بعض المشكلات المحتملة، خصوصاً عند وجود تعارض بين هذه القوانين - وهى من القوانين الخاصة - وبين القواعد والنصوص العامة، التى تقرر حماية مصلحة جوهرية (موضوعية أو إجرائية) للأمن الالكترونى. ولدينا فإنه من الأنسب أن يجرى نصوص هذه المواد على النحو التالى :

(1) صدر بتاريخ 2012/8/13م الموافق 25 رمضان 1433هـ

(2) صدر بتاريخ 30 ذى الحجة 1426 هـ الموافق 30 يناير 2006م.

"... ولا يسرى في شأنه أى حكم يتعارض مع أحكامه. بدلاً من النص على أنه: "...
يلغى كل حكم يخالف أو يتعارض مع أحكام هذا المرسوم بقانون".

ثالثاً : مفهوم جرائم الاعتداء على الأمن الإلكتروني :

لم نصادف حتى الآن تعريف محدد لجرائم الاعتداء على الأمن الإلكتروني، ومن ثم
يمكن تعريف هذا النوع من الجرائم، بأنها كافة صور السلوك غير المشرع (الإيجابي أو
السلبى) الذى يمثل اعتداء (بالضرر أو التهديد به) على كافة سبل تأمين وحماية
الشبكة المعلوماتية، وشبكة الاتصالات، ونظام التحكم الإلكتروني، ونظم المعلومات،
وعمليات جمع المعلومات، أو ما شابه ذلك، والذى يقرر لها المشرع جزاء جنائى أو
تدبير احترازي.

رابعاً : التمييز بين جرائم الاعتداء على الأمن الإلكتروني وما يتشابه معها :

تتميز جرائم الاعتداء على الأمن الإلكتروني، بأنها اعتداء على أمن
وحماية شبكة الاتصالات، ونظم المعلومات، ونظم للتحكم الإلكتروني
ذاتها. ويتم هذا الاعتداء بصور مختلفة، تمثل خطورة على مصالح متعددة
وهامة. ومن أهم صور هذا الاعتداء الدخول إلى هذه الأنظمة بغير
تصريح، أو بتجاوز حدود التصريح، أو البقاء فيه بصورة غير مشروعة، أو

إلغاء، أو حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو تزوير، هذه الأنظمة، أو غير ذلك من صور السلوك الأخرى المشابهة، التي تمثل اعتداء على نظم التأمين، والحماية لهذه الأنظمة الالكترونية.

ومن ثم، فإن جرائم الاعتداء على الأمن الالكتروني تختلف بذلك عن استخدام نظم المعلومات، وشبكة الاتصالات، ونظم التحكم الالكتروني، كأداة أو وسيلة لارتكاب جرائم أخرى. من ذلك مثلاً إنشاء موقع الكتروني لنشر معلومات بهدف الترويج لإثارة الفتنة، أو الإضرار بالوحدة الوطنية⁽¹⁾. أو بهدف الترويج للأسلحة⁽²⁾، أو نشر معلومات لجماعة إرهابية⁽³⁾، أو الترويج للاتجار بالمخدرات⁽⁴⁾، أو بغرض ارتكاب أفعال جرميه متعلقة بأموال غير مشروعة⁽⁵⁾، أو ما شابه ذلك.

خامساً : خصائص جرائم الاعتداء على الأمن الالكتروني :

يمكن أيجاز أهم الخصائص المميزة لجرائم الاعتداء على الأمن الالكتروني في النقاط التالية :-

- تمثل جرائم الاعتداء على الأمن الالكتروني، تهديدا صارخا على

(1) المادة (24) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (25) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (26) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (35) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(5) المادة (37) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

مصالح أساسية في الدولة، كأمن الدولة، واقتصادها، والنظام العام فيها، والسلم الاجتماعي، وكذلك العلاقات الدولية والإقليمية، لذلك فإن المشرع يعتبر هذه الجرائم من جرائم أمن الدولة⁽¹⁾.

- جرائم الاعتداء على الأمن الإلكتروني، جريمة لها بعد دولي، أي أنها جريمة عابرة للحدود أو الأوطان، تتخطى آثارها، ونتائجها، وأضرارها أكثر من دولة في آن واحد.

- تجمع جرائم الاعتداء على الأمن الإلكتروني بين صفة جرائم الضرر الفعلي وجرائم الخطر، أي التهديد بالضرر المحتمل الوقوع. وهذه الأخيرة هي مرحلة مبكرة من الحماية، يستهدف بها المشرع اعتراض خطوات السلوك الإجرامي قبل أن يفضى إلى الضرر.

- جرائم الأمن المعلوماتي تتم في بيئة رقمية معلوماتية، قوامها النظم البرمجية المعلوماتية الحاسوبية، وأجهزة، ومعدات، وأدوات حاسوبية⁽²⁾، أو رقمية.

- جرائم الاعتداء على الأمن الإلكتروني، يتميز فاعليها أو مرتكبيها

(1) حيث تنص المادة رقم (44) من مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، على أنه "تعتبر الجرائم الواردة في المواد 4، من هذا المرسوم من الجرائم الماسة بأمن الدولة.

(2) أنظر في ذلك : خير/ عبد الناصر محمد محمود فرغلي ، د. محمد عبيد سيف سعيد المسماوي : الإثبات الجنائي بالأدلة ارقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2-4/11/1428هـ - الموافق 12-14/11/2007م، ص 11.

وكذلك الشركاء فيها في أغلب الأحيان بالذكاء⁽¹⁾.

(1) انظر : د. غنام محمد غنام : دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة، مصر، 2010، ص15.

المبحث الثاني

تحديد المصالح محل الحماية الجنائية

أولاً : العناصر محل الحماية الجنائية في مجال الأمن الالكتروني :

تعتبر الحماية الجنائية أحد وأهم أنواع الحماية القانونية بصفة عامة⁽¹⁾، وتتحقق عن طريق القواعد والنصوص التشريعية التي يُجرّم ويُعاقب بمقتضاها المشرع على المساس بمصالح ذات أهمية، وهذه الأخيرة تشمل في نطاق الأمن الالكتروني حماية، وتأمين العناصر التالية:-

(أ) تأمين وحماية الشبكة المعلوماتية :

يتباين مفهوم الشبكة المعلوماتية وفقاً للقانون الإماراتي، فقد عرفها أحياناً بأنها ارتباط بين مجموعتين، أو أكثر من البرامج المعلوماتية، ووسائل تقنية المعلومات التي تتيح للمستخدمين الدخول وتبادل المعلومات⁽²⁾. وفي أحيان أخرى عرفها المشرع الإماراتي بأنها ارتباط بين أكثر من نظام معلومات، وشبكات الاتصالات، والأنظمة الالكترونية أو أي منها

(1) انظر في هذا الصدد د. عبد الفتاح مصطفى الصيفي : القاعدة الجنائية، دراسة تحليلية لها على ضوء الفقه الجنائي المعاصر، دار النهضة العربية، القاهرة، بدون سنة نشر، ص 3 وما بعدها.

(2) راجع : المادة الأولى من مرسوم بقانون اتحادي رقم (5) لسنة 2012م.

للحصول على البيانات والمعلومات وتبادلها⁽¹⁾. وهذا التعريف الأخير أوسع نطاقاً حيث يشمل مصطلح الأنظمة الالكترونية.

(ب) تأمين وحماية شبكة الاتصالات :

شبكة الاتصالات هي منظومة تحتوى على جهاز أو وسيلة اتصال أو أكثر، بهدف نقل أو بث أو تحويل أو استقبال أى من خدمات الاتصالات وذلك بواسطة أى طاقة كهربائية أو مغناطيسية أو إلكترومغناطيسية أو إلكتروكيميائية أو إلكتروميكانيكية، وغير ذلك من وسائل الاتصال⁽²⁾.

(ج) تأمين وحماية نظم المعلومات :

نظم المعلومات وفقاً للتشريع الإماراتى هي أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها، وفقاً للأوامر والتعليمات المخزنة بها، ويشمل فى ذلك جميع المدخلات والمخرجات والبنى التحتية المرتبطة بها⁽³⁾.

(د) تأمين وحماية عمليات جمع المعلومات الالكترونية :

المعلومات الالكترونية وفقاً للتشريع الإماراتى لها مدلولان. إحداهما

(1) المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

(2) المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

(3) المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

ضيق والآخر يحمل دلالة واسعة. وهذا الأخير يشمل أى معلومات يمكن تخزينها، ومعالجتها، وتوليدها، ونقلها، بوسائل تقنية المعلومات، وبوجه خاص الكتابة، والصور، والصوت، والأرقام، والحروف، والرموز، والإشارات، وغيرها⁽¹⁾. أو هى عبارة عن بيانات ومعلومات ذات خصائص إلكترونية فى شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج الحاسب الآلى أو غيرها⁽²⁾. أما المعلومات الالكترونية بالمفهوم الضيق فهى البيانات التى تمت معالجتها، وأصبح لها دلالة سواء كانت مرئية أو صوتية أو مقروءة⁽³⁾. ويؤيد الباحث التعريف الموسع حيث يتضمن مزيد من الحماية لمصالح ذات أهمية بالغة.

ثانياً : منهج المشرع الإماراتى فى تقرير الحماية الفعالة للأمن الالكترونى :

انتهج المشرع الإماراتى فيما يتعلق بسياسة الحماية للأمن الالكترونى، كثير من السبل، وقد كان من أهم هذه السبل، هو إنشاء الهيئة الوطنية للأمن الالكترونى فى دولة الإمارات العربية المتحدة، وسوف نسلط الضوء على هذه الهيئة من خلال النقاط التالية :

-
- (1) راجع : المادة الأولى من مرسوم بقانون اتحادى رقم (5) لسنة 2012م.
(2) المادة رقم (1) من القانون الاتحادى رقم (1) لسنة 2006 فى شأن المعاملات والتجارة الإلكترونية، فى دولة الإمارات العربية المتحدة.
(3) المادة الأولى من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني.

(1) أداة إنشاء الهيئة ومقرها :

أنشئت بموجب أحكام المرسوم بقانون رقم (3) لسنة 2012م، ومقرها الرئيسي مدينة أبوظبي، وهى هيئة عامة تتمتع بالشخصية الاعتبارية، ولها الصلاحيات التنفيذية والرقابية اللازمة وفقا لما حدده هذا المرسوم بقانون، وكذلك واللوائح والقرارات التى تصدر تنفيذا له⁽¹⁾.

(2) أهداف الهيئة واختصاصاتها:

تهدف إلى تنظيم حماية شبكة الاتصالات، ونظم المعلومات، وتطوير وتعديل واستخدام الوسائل اللازمة في مجال الأمن الإلكتروني⁽²⁾. ومن أهم اختصاصاتها الفاعلة أيضاً مكافحة جرائم الحاسب الآلي، والشبكة المعلوماتية، وتقنية المعلومات، وإعداد الخطط لمواجهة أية أخطار، أو تهديدات، أو اعتداءات على الأمن الإلكتروني⁽³⁾.

(3) إدارة الهيئة :

يتولى إدارة الهيئة مجلس إدارة يتكون من عدد من الأعضاء لا يزيد على تسعة ولا يقل عن خمسة، ويصدر بتشكيل مجلس الإدارة قرار من رئيس المجلس الأعلى للأمن الوطنى بناء على ترشيح مستشار الأمن الوطنى،

(1) المادتين (2،3) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

(2) المادة (4) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

(3) المادة (4) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

وتكون مدة العضوية بمجلس الإدارة ثلاث سنوات قابلة للتجديد لمدد مماثلة⁽¹⁾.

(4) الطابع السرى للبيانات والمعلومات المقدمة للهيئة :

وفقاً لنص المادة رقم (10) من المرسوم بقانون اتحادى رقم (3) لسنة 2012، فإنه تعتبر جميع البيانات والمعلومات التى تقدمها الجهات المعنية للهيئة والمتعلقة بمهامها سرية، ولا يجوز للهيئة، أو لأى من العاملين فيها اطلاع أى شخص أو جهة عامة أو خاصة عليها، أو الكشف عنها، أو استخدامها لأى غرض غير تلك التى تحددها اللائحة التنفيذية لهذا المرسوم.

(1) المادة (6) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م.

الفصل الثاني

الحماية الجنائية الموضوعية للأمن الالكتروني

تتعلق الحماية الجنائية الموضوعية للأمن الالكتروني، بمجموعة النصوص القانونية التي يحدد بمقتضاها المشرع صور الفعل أو الامتناع عن الفعل المعتبرة جريمة، والتي تستوجب عقوبة جنائية. وسوف نعالج ذلك وفق الخطة التالية :

المبحث الأول : الأركان العامة لجرائم الاعتداء على الأمن الالكتروني.

المبحث الثاني : الجزاءات الجنائية المقررة لجرائم الاعتداء على الأمن الالكتروني.

المبحث الأول

الأركان العامة لجرائم الاعتداء على الأمن الإلكتروني

تقتضى دراسة الأركان العامة لجرائم الاعتداء على الأمن الإلكتروني، أن نبحث في ماديّات هذه الجرائم، وكذلك طبيعة الركن المعنوي فيها، وسوف يكون ذلك من خلال الخطوة التالية.

المطلب الأول : الركن المادي في جرائم الاعتداء على الأمن الإلكتروني.

المطلب الثاني : طبيعة الركن المعنوي في جرائم الاعتداء على الأمن الإلكتروني.

المطلب الأول

الركن المادي في جرائم الاعتداء على الأمن الإلكتروني

أولاً : صور السلوك غير المشروع المنشئ للاعتداء على الأمن الإلكتروني :

يتحقق الاعتداء على الأمن الإلكتروني، وفقاً لما للتشريع الإماراتي بأي من صور

السلوك غير المشروع الآتية :

- دخول (موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات) بدون تصريح، أو بتجاوز حدود التصريح، أو البقاء فيه بصورة غير مشروعة⁽¹⁾.

- دخول (موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلومات، أو وسيلة تقنية معلومات) بدون تصريح، أو بتجاوز حدود التصريح، أو البقاء فيه بصورة غير مشروعة، إذا ترتب على ذلك إلغاء، أو حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو نسخ، أو نشر، أو إعادة نشر أي بيانات أو معلومات⁽²⁾.

● الدخول بدون تصريح إلى (موقع الكتروني، أو نظام معلومات

(1) المادة (1-2) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (2-2) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

الالكتروني، أو شبكة معلوماتية، أو وسيلة تقنية معلومات) بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية⁽¹⁾. أو إذا تعرضت هذه البيانات أو المعلومات للإلغاء، أو الحذف، أو الإتلاف، أو التدمير، أو الإفشاء، أو التغيير، أو النسخ أو النشر، أو إعادة النشر⁽²⁾.

- دخول (موقع الكتروني) بقصد تغيير تصاميمه، أو إلغائه، أو إتلافه، أو تعديله، أو شغل عنوانه⁽³⁾.

- تزوير (مستند الكتروني) من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية أو المحلية، أو غيرها⁽⁴⁾. أو استعمال المستند المزور مع العلم بتزويره⁽⁵⁾.

- (الحصول أو الاستحواذ أو التعديل أو الإتلاف أو الإفشاء) بغير تصريح لبيانات أى مستند الكتروني، أو معلومات الكترونية، عن طريق الشبكة المعلوماتية أو موقع الكتروني، أو نظام المعلومات الالكتروني، أو وسيلة تقنية معلومات، متعلقة بفحوصات طبية أو تشخيص طبي، أو

(1) المادة (4-1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (4-2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (5) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (6-2،1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(5) المادة (6-3) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

علاج، أو رعاية طبية، أو سجلات طبية⁽¹⁾.

- (إعاقة، أو تعطيل) الوصول إلى شبكة معلوماتية، أو موقع إلكتروني، أو نظام معلومات إلكتروني⁽²⁾.

- التحايل على العنوان البروتوكولي للإنترنت (باستخدام عنوان وهمي، أو عنوان عائد للغير، أو بأي وسيلة أخرى) بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها⁽³⁾.

- الإدخال العمدى وبدون تصريح (برنامج معلوماتي إلى الشبكة المعلوماتية، أو نظام معلوماتي إلكتروني، أو إحدى وسائل تقنية المعلومات) بأن أدى ذلك إلى إيقافها عن العمل، أو تعطيلها أو تدمير أو مسح أو حذف أو إتلاف أو تغيير البرنامج أو النظام أو الموقع الإلكتروني أو البيانات أو المعلومات⁽⁴⁾. أو أي فعل عمدى يقصد به إغراق البريد الإلكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف محتوياته⁽⁵⁾.

- استخدام الشبكة المعلوماتية أو نظام معلوماتي إلكتروني أو إحدى وسائل تقنية المعلومات، للتوصل بغير حق إلى أرقام أو بيانات بطاقة ائتمانية

(1) المادة (7) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (8) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (9) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (10-1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(5) المادة (10-2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

أو الكترونية أو أرقام أو بيانات حسابات مصرفية، أو أى وسيلة من وسائل الدفع الإلكتروني. أو إذا قصد من ذلك الحصول على أموال الغير، أو الاستفادة مما تتيحه من خدمات⁽¹⁾.

- تزوير، أو تقليد، أو نسخ، بطاقة ائتمانية أو بطاقة مدينة، أو أى وسيلة أخرى من وسائل الدفع الإلكتروني، باستخدام إحدى وسائل تقنية المعلومات، أو برنامج معلوماتي. أو قبول التعامل بهذه البطاقات مع العلم بعدم مشروعيتها⁽²⁾.

- الحصول بدون تصريح على رقم سرى أو شفرة أو كلمة مرور أو أى وسيلة أخرى للدخول إلى وسيلة تقنية معلومات، أو موقع الكتروني، أو نظام معلومات الكتروني، أو شبكة معلوماتية، أو معلومات الكترونية. وكذلك كل من (أعد أو صمم أو أنتج أو باع أو اشترى أو استورد أو عرض للبيع أو أتاح) أى برنامج معلوماتي أو وسيلة تقنية معلومات، أو روج بأي طريقة روابط لمواقع الكترونية أو برنامج معلوماتي، أو أى وسيلة تقنية معلومات مصممة لأغراض ارتكاب أو تسهيل أو التحريض على ارتكاب الجرائم المنصوص عليها في المرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات⁽³⁾.

(1) المادة (12) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (13) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (14) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

- الالتقاط أو الاعتراض العمدى وبدون تصريح لأى اتصال عن طريق أى شبكة معلوماتية، أو إفشاء المعلومات المتحصل عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق⁽¹⁾.

- استخدام شبكة معلوماتية، أو نظام معلوماتى الكتروني، أو احدى وسائل تقنية المعلومات، في الاعتداء على خصوصية شخص في غير الأحوال المصرح بها قانوناً بأن أسترى السمع، أو اعتراض، أو سجل أو نقل أو بث أو افشى معادشات أو اتصالات أو مواد صوتية أو مرئية، أو التقط صور للغير، أو نشر أخبار أو مشاهدات أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية⁽²⁾.

- أى مالك أو مشغل لموقع الكتروني أو شبكة معلوماتية خزن أو أتاح متعمداً أى محتوى غير قانوني، مع علمه بذلك، (أو لم يبادر بإزالة، أو منع الدخول إلى هذا المحتوى) غير القانوني خلال المهلة المحددة في الإشعار الخطي الموجه له من الجهات المختصة⁽³⁾.

يتبين من خلال التحديد التشريعي لصور السلوك غير المشروع المنشئ للاعتداء على الأمن الالكتروني، أن أغلبها يتم بسلوك أو فعل ايجابي، ينهى

(1) المادة (15) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (21) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (39) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

عنه القانون، ويتمثل في حركة عضوية إرادية لتحقيق النتيجة التي يعاقب عليها القانون، كإلغاء، أو حذف، أو تدمير، أو إفشاء، أو إتلاف، أو تغيير، أو نسخ، أو نشر، أو إعادة نشر أي بيانات أو معلومات، وغير ذلك من صور الأفعال التي عرضنا لها سلفاً. وقليل جداً من صور هذا السلوك يتطلب فيه المشرع أن يكون بسلوك سلبي، حتى أن الصورة الوحيدة لهذه الجريمة ورد النص على تجريمها إذا تمت بما يسمى بالسلوك السلبي البسيط، أي الإمتناع.

بيد أنه، من المتصور أيضاً في بعض الحالات، أن يتم الاعتداء على الأمن الإلكتروني بأفعال سلبية أو امتناع أعقبته نتيجة إيجابية ناشئة عن هذا الامتناع⁽¹⁾.

ومن ثم يفترض المكن المادى فى هذه الجرائم امتناعاً أعقبته نتيجة إجرامية⁽²⁾. من ذلك مثلاً إحجام أو امتناع الجهة أو الشخص عن اتخاذ سبل تأمين وحماية الشبكة المعلوماتية، أو شبكة الاتصالات، أو نظم المعلومات، إذا ترتب على ذلك أضرار أو أخطار معينة، تهدد المصالح ذات الأهمية.

(1) وهو نوع من الجرائم يتوسط الجرائم الإيجابية، والجرائم السلبية. راجع فى هذا الصدد : د. أحمد شوقى عمر أبو خطوة : شرح الأحكام العامة لقانون العقوبات، الجزء الأول، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، 1999، ص 172 وما بعدها.

(2) أنظر : د. محمود نجيب حسنى : جرائم الامتناع والمسئولية الجنائية عن الامتناع، دار النهضة العربية، القاهرة، 1986، ص 1 وما بعدها.

حيث يلزم لانعقاد المسؤولية عن هذه الأفعال أن يكون هناك واجب أو التزام قانوني أو تعاقدى على الجهة أو الشخص المسئول، بشأن التأمين والحماية، وأن يكون لديه إرادة هذا الامتناع، مع توافر علاقة السببية بين الامتناع والنتيجة المعاقب عليها⁽¹⁾.

وهذه الأفعال الأخيرة، وما يلزم لها من ضوابط لانعقاد المسؤولية عنها، على النحو السالف البيان، لم يهتم المشرع الإماراتي بتجريمها، رغم توافر مقومات الجريمة فيها من حيث خطورتها على الأمن الإلكتروني.

ثانياً : طبيعة النتيجة الإجرامية في جرائم الاعتداء على الأمن الإلكتروني :

النتيجة الإجرامية هي الأثر المترتب على السلوك الإجرامي، وهي العدوان الذى ينال المصلحة أو الحق الذى يقرر له القانون حماية جنائية⁽²⁾. وتتميز هذه النتيجة في جرائم الاعتداء على الأمن الإلكتروني، بمظهرين أساسيين، إحداهما يمثل ضرر بالمصلحة، والآخر يمثل ثمة خطر، وفيما يلي بيان ذلك :

(أ) النتيجة الإجرامية في جرائم الاعتداء بالضرر الإلكتروني :

توجد طائفة من جرائم الاعتداء على الأمن الإلكتروني، المنصوص عليها في القانون الإماراتي، يتطلب المشرع في نتيجهتها الإجرامية وجود ضرر

(1) أنظر : د. محمود نجيب حسنى : المرجع السابق، ص 6 وما بعدها.

(2) د. احمد شوقي عمر أبو خطوة : شرح الأحكام العامة لقانون العقوبات، المرجع السابق، ص 226.

فعلي، أو تغير مادي في العالم الخارجي، تدركه الحواس، يصيب المصلحة محل الحماية الجنائية⁽¹⁾. ولكن رغم ذلك يتميز هذا الضرر بأنه يقترب أحياناً من الضرر المعنوي للمصلحة. من ذلك مثلاً جريمة إلغاء، أو حذف، أو تدمير، أو إتلاف، أو تغيير، موقع الكتروني، أو نظام معلومات الكتروني⁽²⁾، أو بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية⁽³⁾. وهذه الجرائم لا تنعقد فيها المسؤولية وتوقيع العقاب، إلا بتحقيق النتيجة الإجرامية التي تطلبها المشرع بالنص القانوني.

(ب) النتيجة الإجرامية في جرائم تعريض الأمن الالكتروني للخطر :

الغالب في القانون العام هو تجريم النتائج الضارة، أما تجريم النتائج الخطرة فأمر نادر⁽⁴⁾، وعلى العكس من ذلك تغلب النتائج الخطرة في كثير من صور جرائم الاعتداء على الأمن الالكتروني. ويميز الفقه الجنائي في نطاق جرائم الخطر بوجه عام بين نوعين هما (جرائم التعريض للخطر المجرد، وجرائم التعريض للخطر الواقعي)⁽⁵⁾.

(1) أنظر حول مفهوم النتيجة الإجرامية. د. أحمد شوقي عمر أبو خطوه : المرجع السابق، ص 227 وما يليها.

(2) المادة (2-2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (1-4) مرسوم بقانون اتحادى رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(4) د. محمود محمود مصطفى : الجرائم الاقتصادية في القانون المقارن، الجزء الأول، الأحكام العامة والإجراءات الجنائية، الطبعة الثانية، القاهرة، 1979، ص 105.

(5) راجع في هذا الصدد: د. أحمد شوقي عمر أبو خطوه : جرائم التعريض للخطر العام، دراسة مقارنة، دار النهضة العربية، القاهرة، 1999، ص 29 وما بعدها.

ومن أمثلة جرائم الخطر الواقعي، في نطاق الاعتداء على الأمن الإلكتروني، جريمة الإدخال العمدى وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية، أو نظام معلوماتي الإلكتروني⁽¹⁾. وجريمة تزوير (مستند إلكتروني) من مستندات الحكومة الاتحادية أو المحلية⁽²⁾. وجريمة تزوير، أو تقليد، أو بطاقة انتمائية، أو أية وسيلة أخرى من وسائل الدفع الإلكتروني، باستخدام إحدى وسائل تقنية المعلومات، أو برنامج معلوماتي⁽³⁾. وجريمة استخدام الشبكة المعلوماتية، للتوصل بغير حق إلى أرقام أو بيانات بطاقة انتمائية أو الكترونية أو أرقام أو بيانات حسابات مصرفية⁽⁴⁾. فهذه الجرائم يمثل قدر التغير الذي أحدثته النتيجة قدر واضح نوعاً.

ومن أمثلة جرائم الخطر المجرد في نطاق الاعتداء على الأمن الإلكتروني، جريمة دخول موقع إلكتروني، أو نظام معلومات إلكتروني، أو شبكة معلومات، بدون تصريح، أو بتجاوز حدود التصريح، أو البقاء فيه بصورة غير مشروعة⁽⁵⁾. فقد نص المشرع الإماراتي صراحة على أن كل من أدخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة أو نظام

(1) المادة (10-1) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (6-2،1) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (13) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (12) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(5) المادة (2-1) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

معلوماتي، (حتى ولو لم تتحقق النتيجة)، وهي إيقاف أو تعطيل أو حذف أو إتلاف البرنامج أو النظام أو الموقع الإلكتروني⁽¹⁾.

وترتيباً على ما سلف ذكره من أمثلة، يتبين أن المشرع الإماراتي لا يعاقب على هذه الجرائم بوصف الشروع، وإنما بوصفها جرائم تامة قائمة بذاتها⁽²⁾. والهدف من العقاب على هذه الجرائم وفقاً لما لاحظته الفقه الجنائي، هو منع وقوع النتائج الضارة، أو اعتراض سبيل خطوات السلوك الإجرامي قبل أن يفضي إلى الضرر الفعلي المحقق الوقوع الذي يصيب المصلحة محل الحماية⁽³⁾. وهي مرحلة مبكرة ومتقدمة من الحماية.

ثالثاً : علاقة السببية في جرائم الاعتداء على الأمن الإلكتروني :

(أ) صعوبة البحث في علاقة السببية ودور القاضي في التثبت منها :

لا يكفي لقيام لتوافر جريمة الاعتداء على الأمن الإلكتروني، وانعقاد المسؤولية الجنائية عن نتيجتها سلوك ونتيجة فحسب، بل يلزم وجود علاقة سببية تربط بينهما. ولا يثير البحث في علاقة السببية على أساس فكرة الضرر، ذات الصعوبات التي نصادفها ونحن بصدد جريمة من جرائم تعريض الأمن الإلكتروني للخطر، ذلك لأنه لم تتحقق بالفعل النتيجة

(1) (المادة رقم 10 من القانون 5 لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات).

(2) د. محمود محمود مصطفى : الجرائم الاقتصادية في القانون المقارن، المرجع السابق، ص 105.

(3) انظر : د. أحمد شوقي عمر أبو خطوة : جرائم التعريض للخطر، المرجع السابق، ص 5 وما بعدها.

الإجرامية حتى يمكن القطع والجزم بفاعلية السلوك في إحداثها⁽¹⁾، وإنما هناك فقط
ثمة حالة خطر أو ضرر محتمل الوقوع بدرجة كبيرة تهدد المصالح محل الحماية
الجنائية.

ولهذا السبب، يبدو أن الحكم بتوافر الفاعلية السببية بين السلوك والنتيجة في
هذه الجرائم، تقوم على الاحتمال التقديرى والسابق على وقوع النتيجة، متى كان
من الممكن تقييم النشاط بأنه يملك مقومات وقوع النتيجة المحتملة⁽²⁾. وهى بالطبع
سببية كامنة، يتم التوصل إليها وتقدير توافرها على الافتراض المنطقي، ذلك لأن
سلوك الفاعل لم يتولد عنه نتيجة مادية في العالم الخارجي. ومن ثم، فإن المحكمة
تستخلص قيام رابطة السببية من الاحتمال القاطع بفاعلية وصلاحيه السلوك القائم
في إحداث النتيجة التى لم تتحقق. بعكس ذلك في نطاق المسؤولية على أساس فكرة
الضرر الذى تحقق بالفعل، فإن المحكمة تتركن في حكمها على توافر رابطة
السببية على الواقع والمستفاد من كون النتيجة التى تحققت وترتبت فعلاً على

(1) د. مأمون محمد سلامة: قانون العقوبات، القسم العام، الطبعة الثالثة، دار الفكر العربي،
القاهرة، 1990، ص 169.

(2) د. مزهر جعفر عبد السلام : جريمة الامتناع، الطبعة الأولى، الإصدار الأول، دار الثقافة للنشر
والتوزيع، عمان، الأردن، 1999، ص 113، د. عبد المنعم محمد إبراهيم رضوان : موضع الضرر
في البنيان القانوني للجريمة، دراسة تحليلية تأصيلية، رسالة دكتوراه، كلية الحقوق، جامعة
القاهرة، 1994، ص 196.

السلوك المرتكب، وهو الضرر الناشئ عن العمل أو السلوك الإجرامي⁽¹⁾.

(ب) تناسب نظرية السببية الملائمة مع جرائم تعريض الأمن الإلكتروني للخطر:

الواقع أنه يبدو أن الإسناد الموضوعي لنظام المسؤولية الجنائية في نطاق الاعتداء على الأمن الإلكتروني على أساس فكرة (الضرر أو الخطر) يتلاءم مع نظرية السببية الملائمة⁽²⁾. ذلك لأن الحكم بتوافر الفاعلية السببية خصوصاً في مجال المسؤولية على أساس الخطر، يقوم على الاحتمال باعتبار أن النتيجة لم تتحقق فعلاً حتى يمكن القطع والجزم بفاعلية السلوك في إحداثها⁽³⁾.

(1) د. مأمون محمد سلامة : قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 1996، ص 168 وما بعدها ؛ د. عبد المنعم محمد إبراهيم رضوان : المرجع السابق، ص 183 وما بعدها.

(2) ومؤدى نظرية السببية الملائمة أن النتيجة الإجرامية في صورتها الواقعية المحددة هي ثمرة لجميع العوامل التي أسهمت في إحداثها، وأن السلوك الإجرامي لا يعتبر سبباً لوقوع النتيجة إلا إذا تبين أنه صالح إلى إحداثها وفقاً للمجرى العادي للأمر، فيعد سلوك الجاني سبباً في النتيجة ولو ساهمت معه في إحداثها عوامل أخرى سابقة عليه أو معاصرة معه أو لاحقة له، ما دامت هذه العوامل متوقعة ومألوفة، فتكون النتيجة متوقعة وفقاً للمجرى العادي للأمر إذا كانت مألوفة وليست بسبب تدخل عوامل شاذة أو غير مألوفة.

د. محمود نجيب حسنى : علاقة السببية، دار النهضة العربية، القاهرة، 1984، ص 160 ؛

د. أحمد شوقي أبو خطوة : المرجع السابق، ص 234 وما بعدها.

(3) د. مأمون محمد سلامة: المرجع السابق، ص 168؛ د. أحمد شوقي عمر أبو خطوة: جرائم التعريض للخطر العام، المرجع السابق، ص 44.

ونشير هنا، إلى أن نظرية السببية الملائمة حلت محل النظرية التقليدية، وهي نظرية تعادل الأسباب، وهذه الأخيرة تقوم على الحكم اللاحق على تحقيق النتيجة المادية وهو ما لا يتلاءم أبداً وعلى الأقل مع انعقاد المسؤولية على أساس فكرة الخطر أو الضرر المحتمل⁽¹⁾.

وواقع الأمر، أنه بتطبيق معيار السببية الملائمة على المسؤولية الجنائية على أساس فكرة الخطر، يعنى توافر الخطر إذا كان السلوك الذى باشره الجانى قد سبقته أو عاصرته ظروف أو عوامل تجعل من المحتمل وفقاً للسير العادى للأمور وقوع النتيجة، وهى تعريض المصالح لضرر محتمل الوقوع⁽²⁾.

ومن ثم، يتعين على قاضى الموضوع التثبت من توافر علاقة السببية كعنصر هام فى المسؤولية على أساس الضرر المحتمل، أو الخطر الفعلى، بنفس الأساس الذى يرتكن إليه فى إثباتها بين السلوك والنتيجة فى نطاق الضرر الذى تحقق وقوعه فعلاً.

ويعتمد هذا الإثبات على افتراضات منطقية، ولكنها غير مؤكدة، مؤداها أن السلوك الإيجابى أو السلبي الذى ارتكب، من شأنه تعريض المصلحة محل الحماية الجنائية لخطر الإضرار بها⁽³⁾.

(1) د. أحمد شوقى عمر أبو خطوة : المرجع السابق، ص 44.

(2) د. مأمون محمد سلامة : المرجع السابق، ص 169.

(3) د. عبد المنعم محمد إبراهيم رضوان : المرجع السابق، ص 183.

وفي هذا الصدد يرى جانب كبير من الفقه⁽¹⁾، ويؤيده جانب كبير من القضاء⁽²⁾، أن المعيار المعول عليه لقياس التوقع أو الاحتمال والذي تبنى على أساسه صفة الخطورة بصفة عامة، هو معيار (موضوعي وليس شخصي). بمعنى أنه لا ينظر إلى موقف الجانب النفسي لمرتكب الفعل غير المشروع حيال هذا التوقع أو الاحتمال وهل هو توقع فعلاً من عدمه، وإنما يستند معيار هذا التوقع والاحتمال على معيار موضوعي، مناطه الفعل أو الخطأ ذاته.

(1) من هذا الرأي : د. مأمون محمد سلامة : المرجع السابق، ص 169؛ د. محمود نجيب حسنى : علاقة السببية، المرجع السابق، ص 161 وما بعدها؛ د. أحمد شوقي عمر أبو خطوة: جرائم التعريض للخطر العام، المرجع السابق، ص 45.

(2) راجع أحكام القضاء في تأييد المذهب الموضوعي - نقض 8 إبريل سنة 1974 - مجموعة أحكام النقض - س 25، ص 395 ونقض 3 يناير 1980 - مجموعة أحكام النقض - س 31، ص 21.

المطلب الثاني

طبيعة الركن المعنوى في جرائم الاعتداء

على الأمن الالكتروني

يقوم الركن المعنوى للجريمة بصفة عامة على الخطأ، وينقسم الخطأ في النظرية العامة للركن المعنوى للجريمة إلى نوعين هما : (الخطأ العمدى، والخطأ غير العمدى)، وسوف نعالج ذلك في نطاق جرائم الاعتداء على الأمن الالكتروني.

أولاً : المعالجة التشريعية للخطأ العمدى في جرائم الاعتداء على الأمن الالكتروني:

(أ) تطلب العمد أو القصد الجنائي صراحة :

حدد المشرع الإماراتى بموجب بعض النصوص القانونية التى تحمى من مظاهر الاعتداء على الأمن الالكتروني صورة الركن المعنوى صراحة، بأن تطلب العمد صراحة لقيام هذه الجريمة. من ذلك مثلاً جريمة الإدخال العمدى لبرنامج معلوماتى إلى الشبكة المعلوماتية، أو نظام معلوماتى الكترونى، أو إحدى وسائل تقنية المعلومات⁽¹⁾. أو أى فعل عمدى يقصد به إغراق البريد الالكتروني بالرسائل وإيقافه عن العمل أو تعطيله أو إتلاف

(1) المادة (10 - 1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

محتوياته⁽¹⁾، وكذلك جريمة الالتقاط أو الاعتراض العمدى وبدون تصريح لأى اتصال عن طريق أى شبكة معلوماتية⁽²⁾. ومن ثم، يجب الالتزام بهذا التحديد التشريعى لصورة الخطأ المتطلبة لقيام الجريمة.

(ب) تطلب القصد الجنائى أو العمد بطريق غير مباشر :

توجد طائفة من الجرائم الواردة بالمنظومة التشريعية لحماية الأمن الالكترونى فى التشريع الإماراتى، يستفاد منها أن المشرع يتطلب القصد الجنائى كركن معنوى فى هذه الجرائم بطريق غير مباشر، من خلال الألفاظ والمصطلحات الواردة بالنص التجريمى، كأن يتطلب المشرع أن تقع الجريمة مثلاً بسوء نية، أو بطريق الغش، أو اشتراط علم الجاني.

من ذلك مثلاً جريمة الدخول بدون تصريح إلى نظام معلومات الكترونى، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية⁽³⁾. وجريمة دخول (موقع الكترونى) بقصد أو إغائه، أو إتلافه⁽⁴⁾. أو جريمة التحايل على العنوان البروتوكولى للانترنت بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها⁽⁵⁾. ومن أمثلة

(1) المادة (10-2) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (15) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (4-1) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (5) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

(5) المادة (9) مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات.

هذه الجرائم في التشريع الفرنسي، جريمة الدخول إلى نظام الكتروني، ثم البقاء فيه بطريق الغش⁽¹⁾. وهذه العبارات تدل بطبيعتها على تطلب القصد الجنائي.

(ج) القصد الخاص في جرائم الاعتداء على الأمن الالكتروني :

توجد طائفة من الجرائم الواردة بالمرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، يتطلب المشرع الإماراتي فيها قصد خاص يقوم على أساس غاية معينة أو مسار بعيد تسلكه إرادة الجاني أبعد مما هو عليه في القصد العام القائم بالطبع على عنصرى (الإرادة والعلم). من ذلك مثلاً جريمة التحايل على العنوان البروتوكولي للانترنت باستخدام عنوان وهمي، أو عنوان عائد للغير بقصد ارتكاب جريمة أو الحيلولة دون اكتشافها⁽²⁾. وجريمة الدخول بدون تصريح إلى شبكة معلوماتية بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية⁽³⁾. وجريمة دخول موقع الكتروني بقصد تغيير تصميمه، أو إلغائه، أو إتلافه، أو تعديله، أو شغل عنوانه⁽⁴⁾.

(1) المادة رقم (1-323) من قانون العقوبات الفرنسي، المعدلة بموجب القانون رقم (575) لسنة (2004).

Article 323-1 Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45

JORF 22 juin 2004

(2) المادة (9) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (1-4) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

(4) المادة (5) مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات.

وترتيباً على ما سلف، فإن القصد الخاص المتطلب في الجرائم السالفة البيان يلعب دوراً هاماً لاكتمال البنيان القانوني للجريمة، ومن ثم ينهار هذا البنيان بتخلفه ولا يتبقى شئ يسأل عنه الجاني، كما لو تخلفت لديه نية الإلغاء، أو الإتلاف، أو التعديل، في جريمة دخول موقع الكتروني أو نظام معلوماتي في الأمثلة السالفة البيان.

ثانياً : جرائم الاعتداء على الأمن الالكتروني في نطاق الخطأ غير العمدى :

(أ) اتجاهات السياسة الجنائية الحديثة :

يعتبر الخطأ العمدى الصورة الثانية للركن المعنوي في الجريمة، وفي هذا النوع من الخطأ تتجه إرادة الفاعل إلى العمل أو الامتناع دون نتائج، ويكمن الخطأ في هذه الصورة في أن الفاعل لم يتخذ نتائج فعله في اعتباره⁽¹⁾. أى أن مقدار سيطرة الجاني على ماديات الجريمة غير العمدية يكون أقل قدرأً منه في الجرائم العمدية⁽²⁾.

وعلى ضوء ما سلف، فإن السياسة الجنائية الحديثة تتجه إلى تجريم الاعتداء غير العمدى على المصالح محل الحماية الجنائية في نطاق الأنظمة

(1) أنظر : د. عبد العظيم مرسى وزير : شرح قانون العقوبات، القسم العام، الجزء الأول، النظرية العامة للجريمة، الطبعة الرابعة، دار النهضة العربية، القاهرة، 2006، ص 362 وما يليها.
(2) أنظر : د. محمود نجيب حسنى : النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1988، ص 11.

الالكترونية. ولعل السبب في ذلك أن هناك بعض الحالات التي يدخل فيها مرتكب الفعل إلى الأنظمة المعلوماتية قد تكون بغرض الترفيه، ومع ذلك قد ينتج عنها أضراراً خطيرة تلحق بأنظمة المعلومات وخصوصاً ما يتعلق منها بالأمن القومي، أو مصلحة الدولة الاقتصادية، أو علاقاتها الدولية والإقليمية، رغم أن نية الجاني فيها لا تتجه إلى الإضرار أو إعاقة النظام.

(1) موقف المشرع الأمريكي :

اتجه المشرع الأمريكي نحو سياسة تجريم الاعتداء غير العمدى في نطاق بيئة النظم الالكترونية. وقد كان الدافع وراء ذلك قضية " موريتس " حيث تسبب هذا الأخير في إعاقة عدد كبير من أنظمة الحاسبات نتيجة إدخاله برنامجاً خبيثاً إلى شبكة المعلومات، دون أن تتجه نيته إلى إحداث النتيجة، وقد تحملت الحكومة الأمريكية عدة ملايين من الدولارات لإعادة تشغيل هذه الأنظمة⁽¹⁾.

لذلك فقد راعى المشرع الأمريكي هذا الأمر حين قيامه بالتعديلات التشريعية للقانون الفيدرالى لجرائم الحاسبات الآلية في سنة 1996. فقد ميز المشرع الأمريكي بموجب المادة رقم (1030/أ) من القانون المشار إليه بين الدخول المصرح به والتي تكون الجريمة غير عمدية في هذه الحالة،

(1) أنظر : د. نائله عادل محمد فريد قورة : جرائم الحاسب الاقتصادية، دراسة نظرية تطبيقية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2013، ص 229.

والدخول المصرح به إلى نظام الحاسب وفيها تكون الجريمة غير عمدية.

وقد جاء بمضمون تقرير مجلس الشيوخ الأمريكي عام 1996 بخصوص تعديل المواد الخاصة بجرائم الحاسبات الآلية، بأن الدخول غير المصرح به إلى نظام الحاسب الآلي هو سلوك غير مشروع في ذاته، ويجب أن تتقرر المسؤولية لمرتكبه عن الإلتلاف الذي يلحق بالمعلومات أو النظام نتيجة لهذا الدخول سواء اتجهت نية محدثة إلى تحقيقه أو حدث نتيجة خطأ⁽¹⁾.

(2) موقف المشرع الفرنسي :

انتهج المشرع الفرنسي ذات المسار الذي انتهجه المشرع الأمريكي، من حيث تجريم الاعتداء غير العمدى على الأنظمة الالكترونية. فقد نص بمقتضى المادة رقم (1-323) من قانون العقوبات الجديد على تعديل ومحو البيانات، حتى ولو تم ذلك عن طريق الخطأ، أى دون توافر قصد التغيير أو الحذف، ويفترض ذلك في جريمة التداخل أو البقاء في نظام الكترونى بطريق الغش⁽²⁾.

كما يعاقب أيضا بذات المادة على الإلتلاف غير العمدى للمعلومات إذا كان الدخول إلى النظام أو البقاء فيه غير مصرح به (المادة 323 عقوبات

(1) Senate Report No 104-357 . 104 th Congress , 2 nd Session Detailed discussion of The NII Protection Act (1996).

(2) أنظر : د. غنام محمد غنام : دور قانون العقوبات في مكافحة جرائم الكمبيوتر، المرجع السابق، ص 153.

فرنسي المعدلة بموجب القانون الصادر سنة 2004⁽¹⁾. ومن ناحية أخرى، يشدد المشرع الفرنسي العقاب إذا ترتب على الدخول غير المصرح محو أو تعديل للمعلومات أو إفساده. والجدير بالإشارة إليه أن الخطأ غير العمدى ينصرف إلى إتلاف المعلومات، أما الدخول والبقاء غير المصرح به داخل النظام يجب أن يكون عمدياً.

(3) موقف المشرع الإماراتي:

إن الملاحظ على المشرع الإماراتي أنه لم ينص صراحة على تطلب الخطأ غير العمدى لإمكان تحقق الركن المعنوى في جرائم الاعتداء على الأمن الإلكتروني، فالصور الواردة للركن المعنوى في هذه الطائفة من الجرائم لا تخرج عن ثلاث افتراضات. (الأول) إما أن يتطلب المشرع العمد صراحة، و(الثاني) أن يتطلب العمد بطريق غير مباشر، و(الثالث) أن يسكت المشرع عن بيان صورة معينة للركن المعنوى في هذه الجرائم. وإزاء هذا الموقف فإن الفقه الجنائي في التشريعات التي تتشابه مع موقف المشرع الإماراتي، تتجه

(1) Article 323-1 Modifié par Loi n°2004-575 du 21 juin 2004 - art. 45 JORF 22 juin 2004 Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

إلى تفسير ذلك على نحو ثلاث نظريات أساسية⁽¹⁾:-

- النظرية الأولى : ترى أن يكون قصد الشارع المساواة بين الخطأ العمدى والخطأ غير العمدى، في إمكان تحقق الجريمة بأى منهم فتقع الجريمة بمجرد وقوع المخالفة، سواء تعمد الجاني المخالفة، أو وقعت بسبب إهماله أو عدم احتياظه⁽²⁾.
- النظرية الثانية : ترى ضرورة الرجوع إلى الأصل العام في التجريم، الذى يعتبر عدم النص على نوع القصد يمثل العمد ولا عقاب على الإهمال إلا بنص صريح⁽³⁾. إلا في مواد المخالفات التى يستوى فيها العمد مع الخطأ.
- النظرية الثالثة : ترى أن تكون هذه الجرائم من قبيل الجرائم المادية، التى

(1) أنظر في بيان ذلك : د. عبد الرؤوف مهدى : المسئولية الجنائية عن الجرائم الاقتصادية، في القانون المقارن، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1974، ص 168، بند رقم (99). وأنظر أيضاً : د. غنام محمد غنام : الحماية الجنائية للادخار في شركات المساهمة، دار النهضة العربية، القاهرة، 1988، ص 84 وما بعدها.

(2) أنظر : د. محمود محمود مصطفى : الجرائم الاقتصادية في القانون المقارن، المرجع السابق، ص 116؛ د. غنام محمد غنام : المرجع السابق، ص 85.

(3) أنظر : د. عبد الرؤوف مهدى : المسئولية الجنائية عن الجرائم الاقتصادية، المرجع السابق، ص 193، د. أحمد شوقي عمر أبو خطوه : المرجع السابق، ص 342، د. محمود كبيش : المسئولية الجنائية لمراقب الحسابات في شركات المساهمة، دراسات مقارنة في القانونين المصرى والفرنسي، دار النهضة العربية، القاهرة، 1992، ص 75 وما بعدها .

A. Vitu " La protection penal de l'interet public et l'interet des associes dans les societes commerciales et civiles " Rapport presente aux cinquieme journees juridiques Franco-Italienne, Paris , Nancy , 5 – 10 juin 1967.

يستهدف المشرع من خلالها تحقيق أغراض تنظيمية يراها ضرورية لتنظيم المجتمع⁽¹⁾، ومن أجل ذلك لا يتطلب المشرع إثبات العمد أو عدم الحيطة، ويكتفى بمجرد وقوع الفعل المادى الذى يعد دليلاً على خطأ الجاني، ومن ثم لا يحتاج إثبات عنصر الخطأ في جانب الجاني⁽²⁾.

والنتيجة العملية للمساواة بين العمد والخطأ، على النحو السالف البيان، وفقاً لما قرره بعض الفقه الجنائي، هو أنه لا يصح التمسك بالجهل بأحكام هذه القوانين، في الجرائم التى يعاقب فيها على مخالفة أحكام هذا القانون⁽³⁾.

ثانياً : الاتجاهات التشريعية الحديثة نحو وضع قاعدة عامة لتحديد نوع الخطأ :

لم تضع اغلب القوانين العقابية في التشريعات المقارنة خصوصاً التشريعات القديمة، نصوصاً تقرر قاعدة يرجع إليها في حالة عدم بيان صورة الركن المعنوى في نص التجريم⁽⁴⁾.

إلا أن الملاحظ على اغلب المدونات العقابية الحديثة بدأت تتخذ

(1) أنظر : د. مصطفى كامل كيره : الجرائم الاقتصادية، دار النهضة العربية، 1983، ص 171 .
(2) أنظر : د. حسنى أحمد الجندى : القانون الجنائي للمعاملات التجارية، الكتاب الأول، القانون الجنائي للشركات، دار النهضة العربية، القاهرة، 1989، ص 151 .
(3) أنظر في بيان ذلك بالتطبيق على أحكام قانون الشركات. د. غنام محمد غنام : المرجع السابق، ص 85.
(4) د. عبد الرؤوف مهدى : شرح القواعد العامة لقانون العقوبات، القاهرة، 2004، ص 445.

مسارها نحو وضع قاعدة عامة بشأن الحالات التي يسكت فيها المشرع عن التصريح بصورة الركن المعنوي الذي يتطلبه لانعقاد الجريمة.

من ذلك مثلاً قانون العقوبات الفرنسي الجديد المعمول به في مارس 1994، حيث نص بموجب المادة رقم (121-3) المعدلة بالقانون رقم (647- لسنة 2000) على أنه " لا جنائية ولا جنحة بدون توافر قصد ارتكابها"⁽¹⁾. وبذلك لا يعاقب المشرع على عدم الاحتياط أو الإهمال إلا بنص خاص في القانون⁽²⁾.

وفي ذات الاتجاه سار المشرع الايطالي بموجب المادة رقم (42) من قانون العقوبات الايطالي التي تنص على أنه " لا عقاب على فعل يعد في القانون جريمة، ما لم يكن قد ارتكب عمداً، عدا حالات الجريمة المتعدية، أو جريمة الخطأ التي يعينها القانون صراحة"⁽³⁾.

(1) Article 121-3 - Modifié par Loi n°2000-647 du 10 juillet 2000 - art. 1 JORF 11 juillet 2000 . "Il n'y a point de crime ou de délit sans intention de le commettre".

(2) د. شريف سيد كامل : تعليق على قانون العقوبات الفرنسي الجديد، القسم العام، الطبعة الأولى، دار النهضة العربية، القاهرة، 1998، ص 90، بند (50).

(3) Art. 42. Responsabilità per dolo o per colpa o per delitto preterintenzionale. Responsabilità obbiettiva. Nessuno può essere punito per un'azione od omissione preveduta dalla legge come reato, se non l'ha commessa con coscienza e volontà. Nessuno può essere punito per un fatto preveduto dalla legge come delitto, se non l'ha commesso con dolo, salvi i casi di delitto preterintenzionale o colposo espressamente preveduti dalla legge. La legge determina i casi nei quali l'evento è posto altrimenti a carico dell'agente, come conseguenza della sua azione od omissione. Nelle contravvenzioni ciascuno risponde della propria azione od omissione cosciente e volontaria sia essa dolosa o colposa.

المبحث الثاني

الجزاءات الجنائية المقررة لجرائم

الاعتداء على الأمن الإلكتروني

الجزاء هو أثر حتمي لكل جريمة⁽¹⁾، وتدور أهدافه حول ثلاثة محاور أساسية هي : الزجر، والعدالة، والإصلاح⁽²⁾. ولهذا يعرف الفقه الجنائي العقوبة بأنها المظهر القانوني لرد الفعل الاجتماعي إزاء الجريمة⁽³⁾، وتتنوع الجزاءات المنصوص عليها وفقاً للقواعد القانونية التي تحمي الأمن الإلكتروني، في التشريع الإماراتي، وسوف نعالج ذلك على نحو الخطة التالية.

المطلب الأول: منهج اختيار الجزاءات المقررة لجرائم الاعتداء على الأمن الإلكتروني.

المطلب الثاني : تقييم خطة المشرع الإماراتي في تقرير الجزاءات.

(1) د. محمد عيد الغريب : شرح قانون العقوبات القسم العام، النظرية العامة للعقوبة والتدابير الاحترازية، بدون دار نشر، القاهرة، 1999-2000، ص961.

(2) Rotman " L'evolutuion de la pense juridique sur le but de la sanction penale " Melange Ancel , 1975 , 11. p. 163.

(3) د. أحمد عوض بلال : محاضرات في الجزاء الجنائي، دار النهضة العربية، القاهرة، 2000 - 2001، ص6.

المطلب الأول

منهج اختيار الجزاءات المقررة لجرائم الاعتداء

على الأمن الإلكتروني

أولاً: صور الجزاءات المقررة لجرائم الاعتداء على الأمن الإلكتروني :

انتهج المشرع الإماراتي فكرة التنوع في العقوبات، تبعاً لجسامة الجريمة في مجال الاعتداء على الأمن الإلكتروني، وتتمثل مظاهر هذا التنوع في تقرير الجزاءات التالية:

(1) عقوبة السجن المؤقت والغرامة :

انتهج المشرع الإماراتي عقوبة السجن المؤقت والغرامة معاً كجزاء جنائي لبعض صور الاعتداء الشديد على الأمن الإلكتروني. من ذلك تقرير عقوبة السجن المؤقت والغرامة التي لا تقل عن مائتين وخمسين ألف درهم، ولا تجاوز مليون وخمسمائة ألف درهم، لكل من دخل بدون تصريح إلى موقع الكتروني، أو شبكة معلوماتية، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية، أو تجارية، أو اقتصادية. إلا أن المشرع رفع الحد الأدنى للعقوبة في هذه الجرائم لعقوبة السجن بحيث لا تقل عن خمس سنوات، والغرامة التي لا تقل عن (500,000) ألف درهم ولا تجاوز (2) مليون درهم، إذا تعرضت هذه البيانات للإلغاء أو الحذف

أو الإتلاف أو التدمير⁽¹⁾.

أضف إلى ذلك فقد انتهج المشرع الإماراتي عقوبة السجن المؤقت وحدها، دون الغرامة، لكل من حصل أو استحوذ أو أتلّف بغير تصريح بيانات مستند إلكتروني أو معلومات إلكترونية، وكانت هذه البيانات تتعلق بفحوصات أو تشخيص طبي⁽²⁾.

كما قيد المشرع الإماراتي أحياناً الحد الأدنى لعقوبة السجن بمدة لا تقل عن خمس سنوات والغرامة التي لا تقل عن خمسمائة ألف درهم ولا تجاوز ثلاثة ملايين درهم، أو بإحدى هاتين العقوبتين، لكل من أدخل عمداً وبدون تصريح برنامج معلوماتي إلى الشبكة المعلوماتية، بأن أدى ذلك إلى إيقافها عن العمل أو تعطيلها⁽³⁾.

(2) عقوبة الحبس والغرامة :

انتهج المشرع الإماراتي عقوبة الحبس والغرامة معاً أو إحداهما، في أغلب صور جرائم الاعتداء على الأمن الإلكتروني، وقد انتهج مبدأ التنوع في مدة الحبس، وكذلك في مقدار الغرامة. من ذلك مثلاً ما تنص عليه المادة رقم (1-2) من قانون مكافحة جرائم تقنية المعلومات التي يعاقب

(1) المادة (4) من مرسوم بقانون اتحادي رقم (5) لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (7) من مرسوم بقانون اتحادي رقم (5) لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات.

(3) المادة (10) من مرسوم بقانون اتحادي رقم (5) لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات.

بمقتضاها بالحبس والغرامة التي لا تقل عن مائة ألف درهم، ولا تزيد على ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، لكل من دخل موقع الكتروني بدون تصريح، أو البقاء فيه بصورة غير مشروعة.

ومن ناحية أخرى، اتجه المشرع الإماراتي نحو تقييد الحد الأدنى لعقوبة الحبس، بحيث لا تقل عن ستة أشهر والغرامة التي لا تقل عن مائة وخمسين ألف درهم ولا تجاوز سبعمائة وخمسون ألف درهم، أو بإحدى هاتين العقوبتين، إذا ترتب على دخول شبكة معلومات بدون تصريح، إلغاء أو حذف أو تدمير أو إفشاء للبيانات أو المعلومات⁽¹⁾.

(3) الظروف المشددة للعقوبة :

يعد ظرفاً مشدداً للعقوبة المقررة لجرائم الاعتداء على الأمن الإلكتروني، وفقاً لما نصت عليه المادة رقم (2-46) من مرسوم بقانون اتحادي رقم (5) لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات، ارتكاب أي جريمة منصوص عليها بموجب هذا المرسوم، لحساب أو لمصلحة دولة أجنبية، أو أي جماعة إرهابية، أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة. كما لا يخل تطبيق العقوبات المنصوص عليها في هذا المرسوم بقانون، بأي عقوبة أشد ينص عليها أيضاً في قانون العقوبات، أو أي قانون آخر⁽²⁾.

(1) المادة (2-2) من مرسوم بقانون اتحادي رقم (5) لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات.

(2) المادة (48) من مرسوم بقانون اتحادي رقم (5) لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات.

والجدير بالإشارة إليه أنه يعتبر ظرفاً مشدداً وفقاً (للقانون الانجليزي)، في جريمة الدخول إلى نظام الكتروني، أو معلوماتي، إذا كانت نية الفاعل تتجه إلى ارتكاب جريمة أخرى أشد من جريمة التدخل، حتى ولو لم تقع هذه الجريمة الأشد، أو كانت جريمة مستحيلة⁽¹⁾. كما يعتبر ظرفاً مشدداً لهذه الجريمة في (القانون الفرنسي) إذا ترتب على ذلك إلغاء، أو تعديل، بيانات مبرمجة في النظام، أو الإخلال بسير النظام⁽²⁾.

(4) حالات تخفيف العقوبة أو الإعفاء منها :

وفقاً لنص المادة رقم (45) من مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، تقضي المحكمة، بناء على طلب من النائب العام، بتخفيف العقوبة أو بالإعفاء منها، عمن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المتعلقة بأمن الدولة وفقاً لأحكام هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم، أو القبض على أحدهم.

(1) Maris Cremona, Jonathan Herring MA, Criminal law, Macmilan, 1998, p.235.

(2) المادة رقم (1-323) من قانون العقوبات الفرنسي المعدلة بموجب القانون رقم (575/ 2004).

(5) العقاب على الشروع :

نص المشرع الإماراتي بموجب المادة رقم (40) من مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، على أنه " يعاقب على الشروع في الجنح المنصوص عليها في هذا المرسوم بنصف العقوبة المقررة للجريمة التامة".

(6) المصادرة :

نص المشرع الإماراتي بموجب المادة (41) من مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، على عقوبة المصادرة، كتدبير عيني وقائي على الأشياء والأدوات التي استعملت في ارتكاب الجريمة، أو كانت محلاً للجريمة الجريمة، أو الأشياء المضبوطة. وقد جاء بهذه المادة السالفة البيان أنه مع عدم الإخلال بحقوق الغير حسنى النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أى من الجرائم المنصوص عليها في هذا المرسوم بقانون أو الأموال المتحصلة منها، أو بمحو المعلومات أو البيانات أو إعدامها.

(7) الغلق الكلى أو المؤقت :

غلق المنشأة⁽¹⁾ هو جزاء عيني، ينص المشرع عليه غالباً كعقوبة تكميلية، إلى جانب ما يقضى به من عقوبات أصلية أخرى⁽²⁾. وقد ورد النص على جزاء الغلق في مجال الاعتداء على الأمن الإلكتروني، بموجب المادة (41) من مرسوم بقانون اتحادي رقم (5) لسنة 2012، حيث يحكم بإغلاق المعلن، أو الموقع الذي يرتكب فيه أي من هذه الجرائم، وذلك إما إغلاقاً كلياً، أو مؤقتاً للمدة التي تقدرها المحكمة.

(8) الحكم بوضع المحكوم عليه تحت الإشراف أو المراقبة :

يجوز للمحكمة وفقاً لنص المادة (42) من مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، أن تأمر بوضع المحكوم عليه تحت الإشراف أو المراقبة أو حرمانه من استخدام أي شبكة

(1) يتمثل غلق المنشأة في المنع من استمرار استغلالها، وقد ثار الجدل حول طبيعتها القانونية حول ما إذا كانت عقوبة خالصة، أم مجرد تدبير احترازي. راجع : د. أمين مصطفى محمد : النظرية العامة لقانون العقوبات الإداري (ظاهرة الحد من العقاب)، دار الجامعة الجديدة للنشر، الإسكندرية، 1996، ص 256.

(2) Merle et vitu : trait de droit criminal , quatrieme edition , 1981 , p. 870.

-A. Wlener, theory of economic criminal law Hungarian national group of international association of penal law Budapest 1984 London 1986, p. 41.

مشار إليهما لدى د. محمود عبد العزيز محمد السيد الشريف : مدى ملائمة الجزاءات الجنائية الاقتصادية في ظل السياسة الجنائية المعاصرة، النظرية العامة للجزاء الجنائي الاقتصادي، دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 2006-2007، ص 103.

معلوماتية، أو نظام المعلومات الالكتروني، أو أى وسيلة تقنية معومات أخرى، أو وضعه فى مأوى علاجى أو مركز تأهيل للمدة التى تراها المحكمة مناسبة.

(9) إبعاد الأجنبى :

نص المشرع الإماراتى على إبعاد الأجنبى بموجب المادة رقم (42) من مرسوم بقانون اتحادى رقم (5) لسنة 2012 فى شأن مكافحة جرائم تقنية المعلومات، بقوله " تقضى المحكمة بإبعاد الأجنبى الذى يحكم عليه بالإدانة لارتكاب أى جريمة من الجرائم المنصوص عليها فى هذا المرسوم، ويكون ذلك بعد تنفيذ العقوبة المحكوم بها".

المطلب الثاني

تقييم خطة المشرع الإماراتي في تقرير الجزاءات

أولاً : تحديد أوجه الإيجابيات المقررة :

يمكن القول أن المشرع الإماراتي ساهم كثيراً بموجب منهج اختيار الجزاءات المقررة لجرائم الاعتداء على الأمن الإلكتروني، في تحقيق كثير من جوانب العدالة، وجبر الضرر، أو الخلل الناشئ عن هذه الجرائم، كما حقق جانب كبير من فكرة الأغراض النفعية للعقوبة، من حيث تحقيق الردع العام والردع الخاص⁽¹⁾.

فقد لجأ المشرع إلى وسائل تفريد العقاب تشريعياً، حيث أنتهج التنويع في العقوبات، تبعاً لجسامة الجرائم إلى حد ما، فقد وضع أكثر من عقوبة أصلية عن الجريمة الواحدة، وتخويل القاضي اختيار إحداها أو الجمع بينهما⁽²⁾.

أضف إلى ذلك فقد نص المشرع على ظروف معينة، إذا ما توافرت أحد حالاتها، يشدد فيها العقوبة. كما وضع المشرع الإماراتي أيضاً العقوبات

(1) أنظر حول أهداف العقوبة : د. عبد الرؤوف مهدي : شرح القواعد العامة لقانون العقوبات، المرجع السابق، ص 965.

(2) أنظر حول تطبيق العقوبة، وسلطة القاضي التقديرية في تطبيقها. د. عبد الرؤوف مهدي : المرجع السابق، ص 1055.

السالبة للحرية، وكذلك مقدار الغرامة المقررة في إطار مرن، حيث قرر لها حد أقصى وحد أدنى، بحيث يستطيع القاضى من خلالها توقيع الجزاء الملائم حسب ظروف الدعوى، وحسب مقدار ما تحدثه الجريمة من خلل أو استهجان⁽¹⁾.

ثانياً : أوجه قصور منهج تقرير الجزاءات الجنائية :

الملاحظ على منهج المشرع الإماراتى في تقرير الجزاءات المقررة على الاعتداء على الأمن الإلكتروني، أنه لم ينص على تشديد بعض العقوبات أو التدابير في حالة (العود للجريمة).

كما لم ينص على ضرورة نشر الحكم الصادر بالإدانة، وهو جزاء يكمل الجزاء الأصلي⁽²⁾، ونادراً ما ينص عليه القانون العام، إلا أن قوانين العقوبات خصوصاً الاقتصادية كثيراً ما تنص عليه⁽³⁾. ويعد القانون الفرنسى وفقاً لما لاحظته أغلب الفقهاء من أكثر التشريعات المقارنة التى تستخدم عقوبة نشر الأحكام الصادرة بالإدانة في نطاق الجزاء المقرر خصوصاً للجرائم الاقتصادية⁽⁴⁾.

(1) راجع في هذا الصدد : د. عبد الرؤوف مهدى : المرجع السابق، ص 1055 وما بعدها.
(2) يتم نشر الحكم الصادر بالإدانة سواء بالشهر على واجهة المحلات، أو بالنشر في الصحف. أنظر في ذلك : د. أمين مصطفى محمد : المرجع السابق، ص 266.
(3) د. محمود محمود مصطفى : الجرائم الاقتصادية، المرجع السابق، ص 176، د. مصطفى منير : جرائم إساءة استعمال السلطة الاقتصادية، الهيئة المصرية العامة للكتاب، 1992، ص 321.
(4) المادة رقم (7) من قانون قمع الغش والتدليس في فرنسا، المعدل بموجب القانون الصادر في 10 يناير 1978. وغيرها من أغلب الجرائم الاقتصادية في فرنسا. راجع تفصيلاً : د. مصطفى منير : المرجع السابق، ص 321 وما بعدها.

وأخيراً، لم ينص أيضاً على جزاء فيما يتعلق بالمسؤولية الجنائية عن فعل الغير، وكذلك مسؤولية الأشخاص المعنوية، من خلال النص على تقرير المسئول عن الإدارة الفعلية لمنشأة أو منظمة أو مجموعة أو جمعية أو منظمة أو هيئة غير مشروعة، يثبت ارتكابها مما يعد جريمة من جرائم الاعتداء على الأمن الإلكتروني.

ثالثاً: التطبيق القضائي للجزاء الجنائي المقرر ومدى فاعليته في معالجة أوجه القصور :

يحدد المشرع العقوبة، وفقاً لمبدأ الشرعية، على أساس تناسبها مع ماديات الجريمة، ومدى خطورتها أو ضررها على المجتمع، وليس في مقدور المشرع التكهن بالاعتبارات التي تحدد العقاب العادل والملائم، ومن ثم فإن تحقيق التناسب، والعدالة، والملائمة، لا يكون بين العقوبة والجريمة، وإنما بين العقوبة والعناصر التي ينوقف عليها تحقيق أهدافها، وهي الخطورة الإجرامية، وجسامة الجريمة⁽¹⁾.

ومن هنا تظهر مهمة القاضي الذي يكمل دور المشرع في تحقيق العدالة، وفي تحقيق الجوانب الإنسانية والاجتماعية، لأن القاضي هو أكثر اتصالاً بالظروف والملابسات التي أحاطت بالجريمة⁽²⁾. وهو يسترشد في ذلك وفقاً

(1) د. محمد عيد الغريب : شرح قانون العقوبات، المرجع السابق، ص 1047.

(2) د. محمد عيد الغريب : المرجع السابق، ص 1048.

لما حدده الفقه الجنائي بضابطين أساسيين هما :-

(أ) الضابط الموضوعي :

يتعلق هذا الضابط بمراعاة القضي سلطته التقديرية إزاء المتهم، بمدى جسامة الجريمة، ومدى الاعتداء على الحق محل الحماية القانونية، حيث يراعى القاضي الاعتبارات التي تؤثر في مقدار جسامة الاعتداء، كأسلوب تنفيذ الفعل، ووقته، ومكانه، وكافة ملبساته، وكلها اعتبارات يسترشد بها القاضي في تحديد العدالة عن طريق النطق بالحكم الملائم⁽¹⁾.

(ب) الضابط الشخصي :

ترتكز الضوابط الشخصية على مراعاة القاضي درجة خطورة الإرادة المؤتممة قانوناً، حيث تتفاوت خطورة هذه الإرادة بطبيعتها في الجريمة الواحدة من حالة لأخرى، كما تعد البواعث من أهم العوامل التي تحدد مقدار خطورتها، وبالتالي التأثير في مجال السلطة التقديرية للقاضي عند اختياره للعقوبة الملائمة لجسامة الجريمة⁽²⁾.

(1) د. محمد عيد الغريب : المرجع السابق، ص 1052 ؛ د. أحمد عوض بلال : محاضرات في الجزء الجنائي، دار النهضة العربية، القاهرة، 2000-2001، ص 330 ، د. حاتم بكار : حماية حق المتهم في محاكمة عادلة، دراسة تحليلية تأصيلية انتقادية مقارنة، منشأة المعارف، الإسكندرية، 1997، ص 505 وما بعدها.

(2) د. محمد عيد الغريب : المرجع السابق، ص 1053 ؛ د. أحمد عوض بلال : المرجع السابق، ص 331.

موقف المحكمة الاتحادية العليا الإماراتية من الضوابط الشخصية والموضوعية :

تطبيقاً للضوابط الموضوعية والشخصية السالفة البيان، فقد قضت المحكمة الاتحادية العليا في دولة الإمارات العربية المتحدة، وقد جاء في حكمها أنه مراعاة ظروف المتهم الشخصية، ومن ثم فإن المحكمة تعامله بشئ من الرحمة وتخفف عنه العقوبة إعمالاً للمادة (98) من قانون العقوبات الاتحادي. وكان ذلك بصدد جريمة استخدام بطريق العلانية وسيلة من وسائل تقنية المعلومات في بث دعايات مثيرة لعامة الناس بأن نشر المتهم مقطعاً مصوراً احتوى على عبارات وتهديدات. عن طريق استحداث موقع جديد على (اليوتيوب) بشبكة الانترنت، وبث فيه مقطع فيديو أنتجه للترويج لأفكار من شأنها الإخلال بالآداب العامة وبالنظام العام بإلقاء الرعب والهلع بين الناس⁽¹⁾.

(1) أنظر : حكم المحكمة الاتحادية العليا في دولة الإمارات العربية المتحدة، في القضية رقم (2) لسنة 2012 جزائي أمن دولة، جلسة الاثنين الموافق 26 من مارس سنة 2012. وقد ورد في مضمون هذا الحكم ضمن الوقائع التي عرضت لها المحكمة في الحكم، أن الشاهد وهو والد المتهم ذكر أن ابنه تعرض للاعتداء بطعنات بسلاح أبيض بمدينة دبي قبل حوالي 6 أشهر، وأن القصد من مقطع الفيديو كما ورد في أقوال المتهم هو إنتاج أغنية راب دون قصد نشر الرعب في المجتمع، وحيث أنه بتفريغ القرص المدمج المضبوط الحامل الرقم التسلسلي من طرف الخبير المهندس / ... من الإدارة العامة للأدلة الجنائية وعلم الجريمة، وتضمن بالخصوص صورة يشاهد فيها أشخاص بصدد الاعتداء بالعنف على شخص وكتب على الصورة " ها بكون مصير كل واحد يسب أو يتزعم على "دنجر"، وصورة أخرى تظهر وجه شاب تكسوه الدماء وكتب على الصورة "والله لأعذبه مثل ما عذبت غيره".

الفصل الثالث

الحماية الجنائية الإجرائية للأمن الإلكتروني

تمر إجراءات الحماية الجنائية للأمن الإلكتروني، بثلاث مراحل أساسية. الأولى هي مرحلة التحري والاستدلال، والثانية التحقيق الابتدائي، والثالثة المحاكمة، وسوف نركز على أوجه الخروج عن القواعد العامة في هذه الإجراءات، في نطاق حماية الأمن الإلكتروني.

المبحث الأول : ذاتية قواعد التحري والاستدلال بشأن الاعتداء على الأمن الإلكتروني.

ذاتية إجراءات التحقيق الابتدائي بشأن الاعتداء على الأمن الإلكتروني.

ذاتية إجراءات المحاكمة بشأن الاعتداء على الأمن الإلكتروني.

المبحث الثاني: المبحث الثالث :

المبحث الأول

ذاتية قواعد التحرى والاستدلال

بشأن الاعتداء على الأمن الالكتروني

تقوم الضبطية القضائية بالبحث عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق والدعوي⁽¹⁾. فعملها لا يبدأ إلا بعد وقوع الجريمة، وبقصد الوصول إلى معاقبة فاعلها، وهي بالطبع تختلف عن الضبطية الإدارية، وهذه الأخيرة مهمتها منع وقوع الجرائم⁽²⁾. وسوف نعالج ذلك في مجال الاعتداء على الأمن الالكتروني في النقاط التالية :

أولاً: تحديد ضبطية قضائية خاصة للتحرى والاستدلال :

تتجه السياسة الجنائية الحديثة في التشريعات المقارنة، ومنها المشرع الإماراتي، إلى تخصيص ضبطية قضائية خاصة تعنى بالبحث والتحري والاستدلال عن الجرائم الالكترونية، وتجد هذه السياسة مبرراتها في أن هذه الجرائم بطبيعتها معقدة، وتحتاج إلى دراية فنية خاصة في الكشف عنها⁽³⁾.

(1) المادة رقم (21) من قانون الإجراءات الجنائية المصري.

(2) أنظر : د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، الطبعة الثانية عشرة، القاهرة، 1988، ص 207، بند (156).

(3) راجع في هذا الصدد : د. محمود محمود مصطفى : الجرائم الاقتصادية في القانون المقارن، مرجع سابق، ص 226.

وفيما يلي بيان منهج المشرع الإماراتي :

(1) أداة منح صفة الضبطية القضائية الخاصة :

الضبطية القضائية الخاصة هم من يقومون بوظيفة الضبطية في جرائم معينة تتعلق عادة بالوظائف التي يؤدونها، فليس لهم مباشرتها خارج هذا النطاق⁽¹⁾. وقد منح المشرع الإماراتي صفة الضبطية القضائية الخاصة لبعض الموظفين لدى الجهات الاتحادية، أو المحلية، المعنية بشؤون الأمن الإلكتروني في الدولة، وقد قرر المشرع أن منح هذه الصفة يكون بقرار من وزير العدل، بالاتفاق مع رئيس مجلس إدارة الهيئة الوطنية للأمن الإلكتروني⁽²⁾.

(2) الجزاء الإجرائي المترتب على مباشرة الضبط العام للمهام المسندة إلى الخاص:

جرى العمل على أن أصحاب صفة الضبطية القضائية العام، لا يباشرون وظيفة الضبطية القضائية الخاصة، ولكن رغم ذلك فإن مباشرتهم لها وفقا لرأي البعض من الفقه ووفقا لما يؤيده الباحث يكون صحيحا⁽³⁾.

(1) أنظر : د. محمود محمود مصطفى : المرجع السابق، ص 209، بند (160).

(2) راجع المادة رقم (1) من مرسوم بقانون اتحادي رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني. والمادة الأولى من مرسوم بقانون اتحادي رقم (5) لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات، في دولة الإمارات العربية المتحدة.

(3) أنظر في ذلك : د. محمود محمود مصطفى : المرجع السابق، ص 210، بند (160).

ذلك لأنه لا يوجد نص يحظر ذلك، كما لا يوجد نص بموجب قانون إنشاء الهيئة الوطنية للأمن الإلكتروني، أو بموجب قانون مكافحة جرائم تقنية المعلومات، في التشريع الإماراتي يقرر بموجبه المشرع اختصاص استثنائي لأعضاء الضبطية القضائية الخاصة، لذلك لا يترتب على مخالفة قواعد هذا الاختصاص بطلان الإجراءات.

(3) نطاق وحدود اختصاص عضو الضبط القضائي :

أكد المشرع الإماراتي بموجب المادة رقم (14) من مرسوم بقانون اتحادي رقم (3)، على أنه يتحدد نطاق اختصاص الهيئة، فيما يلزم لتفادي الاعتداء على الأمن الإلكتروني، سواء كان ذلك من داخل دولة الإمارات، أو من خارجها. وهذا الاتجاه محمود من قبل المشرع الإماراتي، لكون أن أغلب جرائم الاعتداء على الأمن الإلكتروني ترتبط بأماكن وأجهزة وأنظمة عديدة قد تتعدى حدود الدولة الواحدة.

(4) واجبات ومهام وسلطات أعضاء الضبطية القضائية الخاص :

يرى البعض من الفقه أن رجل الضبط القضائي له أن يدخل الأماكن العامة على شبكة الانترنت التي للشخص العادي أن يدخلها كالمواقع المختلفة، وتصح الإجراءات ويجوز الاستناد إليها كدليل، بيد أنه ليس لرجل الضبط أن يستعين ببرامج اختراق الدخول إلى المواضع الخاصة،

(كالإميل والماسنجر)⁽¹⁾...الخ.

ويأتى هذا الرأى متوافقاً فيما قضى به القضاء الفرنسى بأن لرجل الضبط أن يتصل بشبكة الميناتل، وأن يقرأ ما عليها من رسائل دون تعديل في تجهيزها شأنه في ذلك شأن الشخص العادي⁽²⁾. وفي هذا الصدد فقد أوجب المشرع الإماراتى على السلطات المحلية بدولة الإمارات العربية المتحدة، تقديم التسهيلات اللازمة لأعضاء الضبطية القضائية الخاصة⁽³⁾. وهذا الاتجاه ضرورى ولازم للبحث والتحرى والكشف عن الجرائم الالكترونية، نظرا لخطورتها.

ثانياً : آليات وسبل تحقيق الأمن الالكترونى في القانون الإماراتى :

يستفاد مما نصت عليه المادتين أرقام (13-14) من المرسوم بقانون اتحادي رقم (3) لسنة 2012، أن سبل تحقيق الحماية للأمن الإلكتروني في الحالات العادية، يكون عن طريق تدخل السلطات أو الجهات المختصة⁽⁴⁾

(1) أنظر هذا الرأى : د. غنام محمد غنام : المرجع السابق، ص 173.

(2) Crim.25 oct. 2000, Bull. Crim. No 317; Penal 2001. Comm. 27, obs. Maron.

(3) المادة (49) من مرسوم بقانون اتحادي رقم (5) لسنة 2012م، في شأن مكافحة جرائم تقنية المعلومات.

(4) الجهات المختصة أو الجهات المعنية بهذا الشأن وفقاً للقانون الإماراتى هي الجهات الاتحادية، أو المحلية المعنية بشؤون الأمن الإلكتروني داخل الدولة، أو غير ذلك من الجهات التي يصدر بتحديدتها قرار بعد ذلك. راجع المادة الأولى من مرسوم بقانون اتحادي رقم (3) لسنة 2012، والمادة الأولى من مرسوم اتحادي رقم (5) لسنة 2012.

باتخاذ أيًا من الإجراءات التالية :

(1) مراقبة شبكة الاتصالات ونظم المعلومات :

أجازت المادة رقم (13) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، للجهة المختصة اتخاذ كل ما يلزم لمراقبة عدم تعرض شبكة الاتصالات، ونظم المعلومات في الدولة، لأى عمليات دخول غير مشروعة، أو كشف مواقع الخلل في شبكة الاتصالات ونظم المعلومات.

(2) منع وإعاقة وتعطيل شبكة الاتصالات ومحتوى نظم المعلومات :

ويتم ذلك عن طريق قيام السلطة أو الجهة المختصة بوضع الضوابط اللازمة لمنع أى محاولات تهدف إلى تعطيل، أو تخريب، أو تغيير، أو منع الوصول غير المصرح به للشبكة المعلوماتية، أو شبكة الاتصالات، أو محتوى نظم المعلومات⁽¹⁾.

والجدير بالإشارة إليه أن وسيلة تحقيق الأمن الإلكتروني التي تتم بمعرفة السلطة المختصة، يكون عن طريق استخدام إحدى الوسائل الإلكترونية المتعارف عليها، وهى تشمل بصفة خاصة كل ما يتصل بالتكنولوجيا (الكهرومغناطيسية، أو الكهروضوئية، أو الرقمية، أو مؤتمتة، أو ضوئية)، أو ما شابه ذلك⁽²⁾. أو بمعنى أشمل كل ما يتصل بالتكنولوجيا

(1) راجع المادة رقم (1) والمادة رقم (14) من مرسوم بقانون اتحادى رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني.

(2) راجع : المادة الأولى من مرسوم بقانون اتحادى رقم (5) لسنة 2012م.

الحديثة ويكون ذات قدرات كهربائية أو رقمية أو مغناطيسية أو لاسلكية أو بصرية،
أو كهرومغناطيسية أو مؤتمته⁽¹⁾ أو ضوئية أو ما شابه ذلك⁽²⁾.

(1) الوسيط أو المعاملات الالكترونية المؤتمته هو عبارة عن برنامج أو معاملة أو نظام إلكتروني
لوسيلة تقنية المعلومات تعمل تلقائيا بشكل مستقل، كليا أو جزئيا، دون إشراف أو متابعة أو
مراجعة من أي شخص طبيعي. أنظر في ذلك : المادة رقم (1) من القانون الاتحادي رقم (1)
لسنة 2006 في شأن المعاملات والتجارة الإلكترونية، في دولة الإمارات العربية المتحدة.
(2) المادة رقم (1) من القانون الاتحادي رقم (1) لسنة 2006 في شأن المعاملات والتجارة
الإلكترونية، في دولة الإمارات العربية المتحدة.

المبحث الثاني

ذاتية إجراءات التحقيق الابتدائي

بشأن الاعتداء على الأمن الإلكتروني

يهدف التحقيق إلى التثبت من الأدلة القائمة على نسبة الجريمة إلى فاعل معين، لذلك فإن الدليل القانوني هو ما يستمد من التحقيق، وقد اشترط القانون أن يؤدي هذا الإجراء وفقاً لأوضاع وإجراءات وضمانات معينة، وتشمل أهم إجراءات التحقيق التفتيش وضبط الأشياء المتعلقة بالجريمة، وسماع الشهود، وندب الخبراء⁽¹⁾،... الخ. وسوف نركز على بعض من هذه الإجراءات فقط في مجال جرائم الاعتداء على الأمن الإلكتروني، والتي يثار بشأنها المشكلات، وسيكون معالجة ذلك في النقاط المحددة التالية :

أولاً : حرمة الحياة الخاصة والأمن الإلكتروني :

لا شك أن الرسائل، والمستندات، وأنظمة المعلومات الإلكترونية ومحتوياتها الخاصة، تتعلق بحرمة الحياة الخاصة للأفراد، لذلك فإن مراقبتها وتسجيلها، تخضع بالضرورة للضمانات المقررة بموجب قانون الإجراءات الجزائية الإماراتي، ومنها ضرورة صدور إذن من النيابة، وغيرها من

(1) أنظر : د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، المرجع السابق، ص 207 ، ص 259، ص 272.

ويرى البعض من الفقه أنه رغم اختلاف المراسلات البريدية عن الالكترونية، ونظرا لتعلق هذا الأمر بحرمة الحياة الخاصة، فإنه يتعين أن يتدخل المشرع بنص صريح على سريان ذات الضمانات المقررة بموجب قانون الإجراءات الجزائية فيما يتعلق بالمراسلات البريدية، على المراسلات الالكترونية⁽²⁾.

ونشير في هذا الصدد، أن هناك بعض التشريعات الحديثة بالفعل كالتشريع الأمريكي، سوى بين اعتراض الاتصالات السلكية، والالكترونية⁽³⁾. من حيث كونها تتعلق بحرمة الحياة الخاصة وأن الاعتداء عليها يمثل جريمة. ثانياً : التفتيش والضبط بشأن جرائم الأمن الالكتروني :

إن غاية التفتيش هي الضبط⁽⁴⁾. والتفتيش هو البحث عن الحقيقة في مستودع السر، وقد يشمل هذا الإجراء الأشخاص المتهمين، أو المساكن، أو الأمتعة⁽⁵⁾،.. الخ. ولا يجوز لمأمور الضبط القضائي أن يقوم بالتفتيش بدون

(1) المواد (65-131 إجراءات جزائية اتحادي).

(2) د. غنام محمد غنام : المرجع السابق، ص 191.

(3) 2511, Sec. 119, Part I, Chapter 18 title. (Intentionally intercepts any wire. oral or electronic communication.

(4) أنظر : د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، المرجع السابق، ص 283.

(5) أنظر في ذلك : د. احمد شوقي عمر أبو خطوة : المبادئ العامة في قانون الإجراءات الجنائية، القاهرة، 2011، ص 349 وما يليها.

إذن قضائي، إلا في حالات التلبس⁽¹⁾. كما لا يصح قانوناً هذا الإجراء - وهو من إجراءات التحقيق- إلا لضبط جريمة واقعة بالفعل وترجحت نسبتها إلى متهم معين، كما لا يصح اتخاذ هذا الإجراء لضبط جريمة مستقبلية، ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل⁽²⁾. وسوف نبين هذه الأحكام بالتطبيق على جرائم الاعتداء على الأمن الإلكتروني في النقاط التالية :

(1) البطلان الذاتي للدليل لعدم مراعاة الضمانات الإجرائية في التحقيق :

أحاط المشرع الإماراتي إجراءات ضبط الرسائل، ومراقبة المحادثات السلكية واللاسلكية، وتسجيلها بضمانات جوهرية، من أهمها الحصول على موافقة النائب العام⁽³⁾.

ومن ثم يترتب البطلان على عدم مراعاة أحكام التفتيش والضبط، في هذا النطاق وهو نوع من البطلان الذاتي للإجراء⁽⁴⁾ Nullite substantielles.

(1) المادة (53) من قانون الإجراءات الجزائية الإماراتي.

(2) د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، المرجع السابق، ص 275. وأنظر (نقض أول يناير سنة 1962 مجموعة أحكام النقض، س 13، رقم 5، ص 20)

(3) (م 75 إجراءات جزائية).

(4) البطلان الذاتي : مؤداه أن يترك للقاضي تقدير الأحوال التي يترتب البطلان فيها، وليس المشرع هو الذي يقدر مدى أهمية الشكل الذي خولف. أنظر :

Merle- Vitu, Procedure Penal, 1984, P. 543.

وهناك ما يسمى بالبطلان القانوني، ومؤداه أن تقرير مثل هذا البطلان، لا يكون إلا بنص خاص من المشرع، فلديهم أنه لا بطلان بغير نص. أنظر :

Stefani, Levasseur, Bouloc, Procedure Penal, 1984, P. 689.

ورغم ذلك فإن بطلان التفتيش لا يؤثر على الإجراءات السابقة أو اللاحقة عليه، فتصح إدانة المتهم بناء على أدلة أخرى، ومنها اعترافه إذا توافرت شروط صحته، ولم يكن نتيجة حتمية للتفتيش الباطل⁽¹⁾.

وتطبيقاً لذلك فقد قضت المحكمة الاتحادية العليا في دولة الإمارات، بإدانة متهم بناء على اعترافه بتعمد استعمال وسيلة من وسائل تقنية المعلومات (اليوتيوب على شبكة الانترنت) لإنتاج مقطع فيديو مخيف، حتى يجعل لنفسه حالة تخيف الناس وتبعث في قلوبهم الرعب والهلع والخوف⁽²⁾.

(2) الرضا بالتفتيش في جرائم الأمن الإلكتروني :

بالإضافة إلى حالة الإذن، وحالة التلبس، من المقرر أنه يجوز تفتيش الأشخاص والأماكن - ما لم يكن مسكناً في القانون المصري- استناداً إلى رضا صاحب الحق، وهذه القاعدة وجدت تطبيقاً لها في مجال الاعتداء على الأمن الإلكتروني، من جانب القضاء الأمريكي، بل ذهب إلى أبعد من هذا. فقد قرر هذا القضاء في أحد أحكامه أنه لا يستلزم أن يصدر الرضا من صاحب النظام نفسه، بل يكفي أن يكون من شخص يستعمل هذا النظام، فالعبرة بالاعتقاد على استعمال الجهاز وليس بملكية الجهاز⁽³⁾.

(1) أنظر : د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، المرجع السابق، ص 293. وأنظر كذلك (نقض 22 نوفمبر سنة 1945 مجموعة أحكام النقض المصرية، ص 6، رقم 67، ص 201)

(2) حكم المحكمة الاتحادية العليا، القضية رقم (2) لسنة 2012 جزائي أمن دولة، جلسة الاثنين الموافق 26 من مارس سنة 2012.

(3) United States V. Smith, 27 F. Supp. 2d 111, 16-1115 (C.D. III. 1998).

www.cybercrime.gov/smanual 2002.htm

وأخيراً نشير إلى أن القضاء الأمريكي يسوى بين البريد العادي، والبريد الإلكتروني من حيث الضمانات المتعلقة بالتحقيق، فقد قضى ببطلان الدليل المستمد من دخول رجال الضبط القضائي إلى البريد الإلكتروني للمتهم وحصولهم على دليل لإثبات ارتكاب الجريمة لعدم حصولهم على إذن قضائي، ولعدم توافر رضا صاحب البريد نفسه⁽¹⁾.

ثالثاً : الأحكام الإجرائية الخاصة بالأمن الإلكتروني في التشريع الإماراتي :

تضمن قانون الإجراء الجزائية الإماراتي أحكام خاصة بشأن الاتصالات الهاتفية. فقد نصت المادة (75) إجراءات جزائية اتحادي على أنه " لعضو النيابة العامة... أن يراقب المحادثات السلوكية واللاسلكية متى استوجبت مقتضيات التحقيق ذلك". إلا أنه في مجال تحقيق الأمن الإلكتروني في الحالات الاستثنائية (الطارئة أو المستعجلة) انتهج المشرع سياسة إجرائية يهدف بها تحقيق المصالح الهامة ذات الصلة بالأمن الإلكتروني، وسوف نبين ذلك من خلال النقاط التالية :

(1) U.S. c.Maxwell 45 MJ 406 , 1996; Rene PEPIN, Le statut juridique du cornel au Canada et aux Etats- Unis, www. Lex-electronica. Org/articles/v 2-6/pepin.htm

راجع : د. غنام محمد غنام : المرجع السابق، ص 191.

(أ) آليات تحقيق الأمن الإلكتروني في الحالات الطارئة أو المستعجلة :

(1) تحديد إجراءات وضرورات التدخل الطارئ أو العاجل :

منح المشرع الإماراتي للسلطة المعنية أو المختصة- وهي الهيئة الوطنية للأمن الإلكتروني- في الحالات الطارئة أو المستعجلة بشأن منع الاعتداء على الأمن الإلكتروني، صلاحية (مراقبة، أو اختراق، أو معالجة، أو إلغاء، أو تعطيل، أو حجب شبكة الاتصالات ونظم المعلومات وأجهزة الاتصالات والرسائل الإلكترونية) بأى شخص، أو جهة. إلا أن المشرع الإماراتي حدد ضوابط هذا التدخل، إذا تبين للجهة المختصة أن هذا الشخص، أو الجهة اشترك في أى عمل من شأنه أن يؤثر على الآتي⁽¹⁾:-

- أمن الدولة، أو عقيدتها، أو اقتصادها، أو تراثها أو حضارتها.

- النظام العام، أو السلم الاجتماعي.

- العلاقات الدولية والإقليمية.

- المنشآت الحيوية والجهات العامة أو الخاصة العاملة فيها.

- حياة أو أموال أى شخص متواجد بالدولة.

ويبدو مما سلف أنه بقدر خطورة إجراءات التدخل من حيث شمولها

(1) راجع المادة (2-14) من مرسوم بقانون اتحادي رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني، في دولة الإمارات العربية المتحدة.

لأفعال تتمثل في الاختراق، والمعالجة، والإلغاء، والتعطيل والحجب للنظام، إلا أنه على قدر هذه الخطورة يقابلها أهمية المصلحة المعتدى عليها أيضاً، حيث تتضمن مصالح عليا كآمن الدولة، والنظام العام، والعلاقات الدولية...الخ.

(ب) الضوابط والضمانات الإجرائية لحالات التدخل الطارئ أو العاجل :

لم يترك المشرع الإماراتي صلاحية الهيئة في اختراق، أو إلغاء، أو تعطيل، أو حجب شبكة الاتصالات ونظم المعلومات والرسائل الالكترونية،...وغيرها غلى النحو السالف البيان، دون قيود أو ضمانات، وإنما حدد هذه الأخيرة في الآتي :

(1) استطلاع رأى مستشار الأمن الوطني :

أشار المرسوم بقانون اتحادي رقم (3) لسنة 2012، فيما تضمنته المادة رقم (14)- (2) من هذا المرسوم إلى أنه يلزم للإجراءات التي تتخذ في الحالات الطارئة أو المستعجلة، لمنع الاعتداء على الأمن الالكتروني، استطلاع رأى مستشار الأمن الوطني.

(2) إخطار النيابة العامة المختصة :

تطلبت المادة رقم (2/14) من المرسوم بقانون اتحادي رقم (3) لسنة 2012 أنه في الحالات المستعجلة التي تبرر ضرورات التدخل الطارئ

بالإجراءات السالفة البيان، أن يتم إخطار النيابة العامة المختصة بالإجراء الذي اتخذته الهيئة في هذه الحالات، خلال أسبوع لإعمال شئونها حيال هذا الإجراء⁽¹⁾.

ويبدو أن حالات وضرورات التدخل الطارئ، من قبل الهيئة الوطنية للأمن الإلكتروني، على النحو السالف البيان، هي مسألة تقديرية للهيئة، ولكنها تخضع لرقابة القضاء فيما بعد. أضيف إلى ذلك أن النيابة العامة - وفقاً لمؤدى المادة (14) من القانون (3) لسنة 2012- لها حرية إعمال شئونها حيال الإجراءات التى اتخذتها الهيئة. وهو ما يقرر نوع من الرقابة التى تمارسها النيابة العامة على صحة الإجراءات التى اتخذتها الهيئة.

(1) المادة (2-14) من مرسوم بقانون اتحادي رقم (3) لسنة 2012م، بإنشاء الهيئة الوطنية للأمن الإلكتروني، في دولة الإمارات العربية المتحدة.

المبحث الثالث

ذاتية إجراءات المحاكمة بشأن الاعتداء على الأمن الإلكتروني

أولاً : البعد الدولي لجرائم الاعتداء على الأمن الإلكتروني :

تعتبر جرائم الاعتداء على الأمن الإلكتروني من الجرائم ذات البعد الدولي⁽¹⁾. ذلك لأن أغلب هذه الجرائم، كالدخول إلى موقع الكتروني لإعاقة أو تعطيله، أو الإدخال العمدى لنظام الكتروني، بقصد الحصول على بيانات حكومية، أو معلومات سرية خاصة بمنشأة مالية أو تجارية أو اقتصادية ... الخ. قد ترتكب أو تترتب آثارها، أو نتائجها الخطيرة أو الضارة في مكان آخر، أو في دولة أخرى غير التي ارتكب فيه السلوك، فضلاً عن أنه قد تكون جنسية مرتكبها، أو المجنى عليه فيها أجنبياً.

وهذه المسألة تثير كثير من المشكلات فيما يتعلق بتحديد المحكمة المختصة بنظر الدعاوى الجنائية الناشئة عن هذه الجرائم، إذا ما اتخذت بالطبع بعداً دولياً بسبب جنسية الجاني، أو جنسية المجنى عليه، أو بسبب

(1) أنظر في هذا الصدد : د. غنام محمد غنام : المرجع السابق، ص 204. وهذه الجرائم رغم أنها تتخذ بعد دولي إلا أنها ليست جريمة دولية، لأن هذه الأخيرة لها تعريف لا يرى على هذا النوع من الجرائم، لكون الجريمة الدولية تمس مصلحة جوهريّة للمجتمع الدولي كالجرائم ضد السلام، والجرائم ضد الإنسانية، وجرائم الحرب. أنظر : د. محمود نجيب حسني : دروس في القانون الجنائي الدولي، دار النهضة العربية، القاهرة، 1959-1960، ص 45 وما بعدها.

الإقليم الذي ارتكبت فيه⁽¹⁾.

ثانياً : ضوابط الاختصاص بجرائم الأمن الالكتروني في التشريع الإماراتي:

يفهم الاختصاص بأنه مباشرة المحكمة ولايتها القضائية في نظر الدعوى في الحدود التي رسمها القانون⁽²⁾. ولا تكون المحكمة الجنائية مختصة بنظر الدعوى المرفوعة إليها إلا إذا كانت مختصة بالنسبة لشخص المتهم، ومن حيث نوع الجريمة المسندة إليه، ومن حيث المكان⁽³⁾. ومن المعلوم أيضاً أنه يسود النطاق المكاني لقانون العقوبات مبدأ إقليمية القانون الجنائي، الذي يعنى أن قانون العقوبات يطبق على إقليم الدولة التي أصدرته⁽⁴⁾.

إلا أن المشرع الإماراتي، خرج على هذه القاعدة فيما يتعلق بجرائم الاعتداء على الأمن الالكتروني، وانتهج مبدأ العينية⁽⁵⁾. حيث نص المشرع بموجب المادة رقم (47) من قانون مكافحة جرائم تقنية المعلومات على أنه

(1) أنظر : د. محمد عيد الغريب : المرجع السابق، ص 1107.

(2) د. احمد شوقي عمر أبو خطوة : المبادئ العامة في قانون الإجراءات الجنائية، المرجع السابق، ص 482.

(3) د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، المرجع السابق، ص 351.

(4) د. عبد الرؤوف مهدي : محاضرات في قانون العقوبات الاقتصادي، دار النهضة العربية، القاهرة، 2007-2008، ص 15. وراجع المادة رقم (16) من قانون العقوبات الاتحادي.

(5) مقتضى هذا المبدأ تطبيق القاعدة الجنائية الوطنية على الجرائم التي تمس مصلحة أساسية للدولة، أو تهدد كيانهما أيا كانت جنسية مرتكبها أو مكان وقوعها. أنظر : د. عبد العظيم مرسى وزير : شرح قانون العقوبات، القسم العام، المرجع السابق، ص 100.

"... تسرى أحكام هذا المرسوم بقانون على كل من ارتكب إحدى الجرائم الواردة به خارج الدولة، إذا كان محلها نظام معلوماتي إلكتروني، أو شبكة معلوماتية، أو موقع إلكتروني، أو وسيلة تقنية معلومات خاصة بالحكومة الاتحادية، أو إحدى الحكومات المحلية لإمارات الدولة، أو إحدى الهيئات أو المؤسسات العامة المملوكة لأي منها".

ومن هنا فقد اعتبر المشرع الإماراتي، أن الاعتداء على الأمن الإلكتروني فيما يتصل بالحكومة، أو إحدى الهيئات والمؤسسات العامة، مصلحة أساسية وجوهرية للدولة، تهدد كيائها، لذلك قرر الخروج عن القواعد العامة في شأن مبدأ الإقليمية. ويؤيد علماء القانون الجنائي وبحق هذا الاتجاه بوجه عام خصوصاً في مجال الجرائم الاقتصادية⁽¹⁾.

ثالثاً : صعوبة الإثبات الجنائي في مجال الاعتداء على الأمن الإلكتروني :

(1) ذاتية الدليل الإلكتروني في مجال إثبات الاعتداء على الأمن الإلكتروني :

تتميز الأدلة الإلكترونية، أو ما يطلق عليها البعض أحياناً الأدلة الرقمية، بعدة خصائص من حيث أنها في أغلب الأحيان من الأدلة غير الملموسة، لذلك فإن إدراكها يحتاج إلى الاستعانة بأجهزة، ومعدات، وأدوات، ونظم وبرمجة حاسوبية، كما تتميز هذه الأدلة خصوصاً في ظل

(1) أنظر في بيان ذلك تفصيلاً د. عبد الرؤوف مهدي : المرجع السابق، ص 17. د. السعيد مصطفى السعيد : مجموعة المحاضرات التي ألقى على طلبة الدراسات العليا في الجرائم الاقتصادية، 1967، ص 49.

التقدم التقني بإمكان استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، مما يصعب الخلاص منها، حيث توجد العديد من البرامج الحاسوبية وظيفتها استعادة البيانات بعد الحذف، كما أن الأدلة الرقمية ذات طبيعة ديناميكية فائقة السرعة، تنتقل من مكان لآخر عبر شبكات الاتصال متعددة لحدود الزمان والمكان⁽¹⁾.

وعلى ضوء ما سلف ذكره من خصائص، فإن مظاهر صعوبة إثبات هذه الأدلة، والتعويل عليها في الأحكام القضائية، تكمن في مدى الحاجة إلى أهل الخبرة من الفنين والمتخصصين، ومدى صلاحية الدليل ذاته نظراً لطبيعته الخاصة في تكوين عقيدة القاضي وقناعته الشخصية.

(2) حتمية الاستعانة بالخبرة الفنية في مجال إثبات الاعتداء على الأمن الإلكتروني:

لم تفرض التشريعات المقارنة على القاضي الجنائي ضرورة الاستعانة بأهل الخبرة في مجال الاعتداء على الأمن الإلكتروني. فالقاضي هو الخبير الأعلى⁽²⁾. ومع ذلك فإن الطبيعة المعقدة لجرائم الاعتداء على الأمن الإلكتروني، على نحو ما ذكرنا آنفاً، تفرض وتحتّم على القاضي الاستعانة بأهل الخبرة من المتخصصين.

(1) أنظر: خير/ عبد الناصر محمد محمود فرغلي، د. محمد عبيد سيف سعيد المسماري: المرجع السابق، ص 14 وما يليها.

(2) د. محمود محمود مصطفى: الجرائم الاقتصادية في القانون المقارن، المرجع السابق، ص 86.

وقد وجدت هذه الفكرة تكريسا قضائياً لها في أغلب الأحكام القضائية المتعلقة بجرائم الاعتداء على الأمن الإلكتروني. فقد قررت محكمة النقض الفرنسية في أحد أحكامها أنه من الضروري الاستعانة بأهل الخبرة فيما يتعلق بجرائم تقنية المعلومات⁽¹⁾. وكذلك ما تبين أيضاً من اتجاه حكم المحكمة الاتحادية العليا الإماراتية في أحد أحكامها⁽²⁾. وما سارت عليه اتجاهات أحكام المحكمة الاقتصادية الجنائية في مصر⁽³⁾.

ثالثاً : التعاون الدولي في مواجهة جرائم الاعتداء على الأمن الإلكتروني :

(1) أهمية وضرورة التعاون الدولي :

يرى بعض الفقه الجنائي أنه من الضروري أن يتم تنظيم التعاون الدولي في مجال مكافحة جرائم تقنية المعلومات، بوجه عام، وتشمل مظاهر هذا

(1) حيث أدانت متهم في جريمة استيراد برامج مزيفة ومزورة بالمخالفة لأحكام المادة 3/355 والمادة 3/6/122 الفقرة 1 و 2 من قانون الملكية الفكرية الفرنسي، وبنت المحكمة حكمها على ما انتهى إليه تقرير هذا الخبير، من أن التقليد كان بطريقة توحى للمستهلك بما لا يدع مجالاً للشك، بأن هذا المنتج المزيف هو ذاته المنتج الأصلي. انظر :

Cour de Cassation chambre criminelle Arrêt du 6 février 2001.

(2) حيث ورد في حكمها أنه تم تفريغ القرص المدمج المضبوط الحامل الرقم لسلي سالت GBS 601E 93 D281A80 من طرف الخبير المهندس من الإدارة العامة للأدلة الجنائية وعلم الجريمة.

انظر القضية رقم (2) لسنة 2012 جزائي أمن دولة، جلسة الاثنين الموافق 26 من مارس سنة 2012.

(3) حيث أدانت المتهم بناء على الأدلة المتحصل عليها بالفحص الفني بمعرفة قسم المساعدات الفنية بفحص البريد الإلكتروني لكل من المجنى عليها والمتهم. الدعوى رقم (26) لسنة 2008، جنح كلى اقتصادي، جلسة السبت 31 يناير 2009.

التعاون المساعدة بين أجهزة الضبط، والتحقيق، والمحاكمة، بل من الممكن أن يرقى التعاون إلى إيجاد نوع من التقارب التشريعي في مجال تجريم أفعال الاعتداء على الأمن الإلكتروني⁽¹⁾. وهذه الرؤية بلا شك تفرضها الطبيعة والذاتية الخاصة لجرائم تقنية المعلومات والاتصالات، التي على ما يبدو أصبحت تستقل عن الجرائم العادية، بذاتية موضوعية، وكذلك إجرائية.

(2) عوائق ومشكلات التعاون الدولي :

حدد الفقه الجنائي بعض من عوائق التعاون الدولي في مجال مواجهة جرائم الاعتداء على الأمن الإلكتروني، أو جرائم تقنية المعلومات بوجه عام، وتتمثل أهم مظاهر هذه العوائق من صعوبة معرفة الفاعل في هذه الجرائم أحياناً، بالإضافة إلى وقوع هذه الجرائم غالباً خارج الدولة التي يحدث فيها الاعتداء، حال كون أن هذه الجرائم لا يوجد اتفاق أو توافق بين الدول على تجريم ذات الأفعال، وأخيراً عدم وجود اتفاقيات دولية لتسليم المجرمين في هذا النوع من الإجرام⁽²⁾.

رابعاً : مدى الحاجة إلى قضاء متخصص في مجال جرائم تقنية المعلومات :

تتجه السياسة التشريعية الحديثة إلى مبدأ التخصص القضائي. من ذلك مثلاً المشرع البلاروسي الذي أنشأ المحاكم الاقتصادية، وأسند إليها

(1) أنظر في هذا الرأي : د. غنام محمد غنام : المرجع السابق، ص 218 وما يليها.

(2) راجع : د. غنام محمد غنام : المرجع السابق، ص 219 وما يليها.

الاختصاص والولاية بنظر بعض المنازعات المحددة⁽¹⁾، ومنها جرائم تقنية المعلومات والاتصالات.

وكذلك الشأن في التشريع الفرنسي وفقاً لآخر التعديلات التشريعية الواردة بقانون الإجراءات الجنائية. حيث تنص المادة (704) من قانون الإجراءات الجنائية الفرنسي- المعدلة بالقانون رقم 1598 لسنة 2007 - على أن تنشأ في دائرة كل محكمة استئناف محكمة جنح أو أكثر للتحقيق والحكم في الجرائم المنصوص عليها في بعض القوانين الاقتصادية⁽²⁾. ومنها بالطبع جرائم تقنية المعلومات، وجرائم الملكية الفكرية. وأخيراً فقد تنبه المشرع المصري لمبدأ التخصص القضائي، فأنشأ المحاكم

(1) راجع : قانون المحاكم الاقتصادية لجمهورية روسيا البيضاء الصادر بموجب القانون رقم (217) الصادر في كانون الأول ديسمبر سنة 1998 والذي اعتمده مجلس النواب في الأول من نوفمبر 1998 والذي دخل حيز النفاذ في 26 نوفمبر 1998.

ЗАКОН РЕСПУБЛИКИ БЕЛАРУСЬ от 9 декабря 1998 г. N 217-3 О ХОЗЯЙСТВЕННЫХ СУДАХ В РЕСПУБЛИКЕ БЕЛАРУСЬ Принят Палатой представителей 10 ноября 1998 года Одобрен Советом Республики 26 ноября 1998 года

(2) Article 704-1 En savoir plus sur cet article... Modifié par Loi n°2004-204 du 9 mars 2004 - art. 21 JORF 10 mars 2004 en vigueur le 1er octobre 2004 Le tribunal de grande instance de Paris a seul compétence pour la poursuite, l'instruction et le jugement des délits prévus aux articles L. 465-1 et L. 465-2 du code monétaire et financier. Cette compétence s'étend aux infractions connexes. Le procureur de la République et le juge d'instruction de Paris exercent leurs attributions sur toute l'étendue du territoire national.

الاقتصادية الجنائية بموجب القانون رقم 120 لسنة 2008، لتختص دون غيرها بنظر منازعات بعينها⁽¹⁾، ووفقاً لما نصت عليه المادة رقم (4) من قانون إنشائها فإن اختصاصها يشمل نظر الدعاوى الجنائية الناشئة عن قانون تنظيم التوقيع الإلكتروني، وقانون تنظيم الاتصالات.

ونأمل من المشرع الإماراتي أن ينتهج مبدأ التخصص القضائي في مجال جرائم تقنية المعلومات والاتصالات، وغيرها من الجرائم ذات الصلة أو المرتبطة بهذه الجرائم. حيث لا تثير فكرة إنشاء قضاء متخصص ثمة مشكلات قانونية، إذا راعى المشرع في قانون إنشائها، توافق هذه المحاكم واختصاصها مع المبادئ والقواعد الدستورية، بحيث يكون إنشائها بناء على قانون، وأن تتوافق مع مبدأ وحدة واستقلالية القضاء، بل ونؤكد هنا أن التخصص القضائي يأتي متوافقاً مع ما جرت عليه توصيات مؤتمر روما قديماً منذ سنة 1953 الذي حث ضمن توصياته على أن يراعى المشرع في كل محكمة تخصيص عدد من قضاتها لمسائل معينة⁽²⁾.

(1) القانون رقم 120 لسنة 2008 بإصدار قانون إنشاء المحاكم الاقتصادية في مصر، الجريدة الرسمية، العدد 21 تابع في 22 مايو 2008.

(2) راجع : مجموعة المناقشات والقرارات الصادرة عن المؤتمر الدولي السادس لقانون العقوبات، المجلة الدولية لقانون العقوبات، سنة 1953، ص 300 وما بعدها.

الختام

حاولنا من خلال هذه الدراسة التعرف على جرائم الاعتداء على الأمن الإلكتروني، وخطورتها، وانعكاساتها المختلفة، وكذلك استكشاف أوجه قصور قواعد الحماية الجنائية بشقيها (الموضوعي والإجرائي) في هذا المجال الحيوي، بهدف التوصل إلى رسم معالم النموذج التشريعي الأمثل للمصالح محل الحماية الجنائية. وقد خلصنا من خلال هذه الدراسة إلى التوصيات التالية :-

- (1) من المناسب، أن يجرى نص المادة رقم (50) من مرسوم بقانون اتحادي رقم (5) لسنة 2012 في شأن مكافحة جرائم تقنية المعلومات، وكذلك نص المادة رقم (23) من مرسوم بقانون اتحادي رقم (3) بشأن إنشاء الهيئة الوطنية للأمن الإلكتروني على النحو التالي " لا يسرى في شأن هذا القانون أى حكم يتعارض مع أحكامه ". بدلاً من النص على أنه " يلغى كل حكم يخالف، أو يتعارض مع أحكام هذا المرسوم بقانون". حتى يتحقق الموازنة التشريعية خصوصاً عند وجود تعارض محتمل بين هذه القوانين - وهي من القوانين الخاصة - وبين القواعد أو النصوص العامة، التي تقرر ذات الحماية لمصلحة جوهرية (موضوعية أو إجرائية) للأمن الإلكتروني.

(2) من الملائم، أن ينص المشرع الإماراتي على تجريم صور الاعتداء على الأمن الإلكتروني التي تتم عن طريق الامتناع الذي تعقبه نتيجة ايجابية ناشئة عن هذا الامتناع من ذلك مثلاً إحجام أو امتناع الجهة أو الشخص عن اتخاذ سبل تأمين وحماية الشبكة المعلوماتية، أو شبكة الاتصالات، أو نظم المعلومات، إذا ترتب على ذلك أضرار أو أخطار معينة، تهدد المصالح ذات الأهمية. مع مراعاة النص على الشروط والضوابط الأخرى لانعقاد المسؤولية عن هذه الأفعال، كأن يكون هناك واجب أو التزام قانوني أو تعاقدى على الجهة أو الشخص المسئول، بشأن التأمين والحماية، وأن يكون لديه إرادة هذا الامتناع، مع توافر علاقة السببية بين الامتناع والنتيجة المعاقب عليها.

(3) من الضروري، أن يحصر المشرع الإماراتي تطلب القصد الخاص في جرائم الاعتداء على الأمن الإلكتروني في أضيق الحدود، فالنص على ضرورة وجود غاية معينة أو مسار بعيد تسلكه إرادة الجاني أبعد مما هو عليه في القصد العام، كثيراً ينهار به البنيان القانوني للجريمة بتخلفه، ولا يتبقى شيء يسأل عنه الجاني، كما لو تخلفت لديه نية الإلغاء، أو الإتلاف، أو التعديل، في جريمة دخول موقع الكتروني أو نظام معلوماتي.

(4) من الملائم، أن يتبع المشرع الإماراتي ذات المسلك الذي تتجه إليه أغلب التشريعات الحديثة، بشأن النص صراحة على تجريم الاعتداء غير

العمدى على المصالح محل الحماية الجنائية في نطاق الاعتداء على الأمن الإلكتروني، ذلك لأن هناك بعض الحالات التي يدخل فيها مرتكب الفعل إلى الأنظمة المعلوماتية وقد تكون (بغير عمد)، ومع ذلك ينتج عنها أضرار جسيمة، تلحق بأنظمة المعلومات وخصوصاً ما يتعلق منها بالأمن القومي، أو مصلحة الدولة الاقتصادية، أو علاقاتها الدولية والإقليمية، على أن يركز المشرع بصفة خاصة على تجريم حالات (الخطأ الواعى أو الخطأ مع التوقع أو مع التبصر)، حيث يتوقع الجاني حدوث النتيجة بدرجة كبيرة عما هو عليه الشأن في (الخطأ غير الواعى).

(5) من المناسب، في تقرير الجزاءات المقررة لجرائم الاعتداء على الأمن الإلكتروني، أن ينص المشرع الإماراتي على تشديد بعض العقوبات أو التدابير في حالة (العود للجريمة). وكذلك النص على ضرورة نشر الحكم الصادر بالإدانة.

(6) من الملائم، أن ينتهج المشرع الإماراتي مبدأ التخصص القضائي في مجال جرائم تقنية المعلومات والاتصالات، وما يرتبط بها من جرائم لا تقبل التجزئة، وذلك على نهج ما سارت عليه أغلب التشريعات المقارنة، كالتشريع البيلاروسي، والمشرع الفرنسي، والمشرع المصري.

المراجع

أولاً : المراجع العربية :

(أ) المؤلفات العامة :

- د. احمد شوقي عمر أبو خطوة :
 - المبادئ العامة في قانون الإجراءات الجنائية، القاهرة، 2011.
 - شرح الأحكام العامة لقانون العقوبات، الجزء الأول، النظرية العامة للجريمة، دار النهضة العربية، القاهرة، 1999.
- د. عبد الرؤوف مهدى : شرح القواعد العامة لقانون العقوبات، القاهرة، 2004.
- د. عبد العظيم مرسى وزير : شرح قانون العقوبات، القسم العام، الجزء الأول، النظرية العامة للجريمة، الطبعة الرابعة، دار النهضة العربية، القاهرة، 2006.
- د. مأمون محمد سلامة : قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 1996.
- د. محمد عيد الغريب : شرح قانون العقوبات القسم العام، النظرية العامة للعقوبة والتدابير الاحترازية، بدون دار نشر، القاهرة، 1999-2000.

- د. محمود محمود مصطفى : شرح قانون الإجراءات الجنائية، الطبعة الثانية عشرة، القاهرة، 1988.
- (ب) المؤلفات الخاصة :
- د. أحمد شوقي عمر أبو خطوة : جرائم التعريض للخطر العام، دراسة مقارنة، دار النهضة العربية، القاهرة، 1999.
- د. أحمد عوض بلال : محاضرات في الجزاء الجنائي، دار النهضة العربية، القاهرة، 2000 - 2001.
- د. السعيد مصطفى السعيد : مجموعة المحاضرات التي أقيمت على طلبه الدراسات العليا في الجرائم الاقتصادية، 1967.
- د. أمين مصطفى محمد : النظرية العامة لقانون العقوبات الإداري (ظاهرة الحد من العقاب)، دار الجامعة الجديدة للنشر، الإسكندرية، 1996.
- د. حاتم بكار : حماية حق المتهم في محاكمة عادلة، دراسة تحليلية تأصيلية انتقادية مقارنة، منشأة المعارف، الإسكندرية، 1997.
- د. حسنى أحمد الجندي : القانون الجنائي للمعاملات التجارية، الكتاب الأول، القانون الجنائي للشركات، دار النهضة العربية، القاهرة، 1989.

- د. شريف سيد كامل : تعليق على قانون العقوبات الفرنسى الجديد، القسم العام، الطبعة الأولى، دار النهضة العربية، القاهرة، 1998.
- د. عبد الفتاح مصطفى الصيفى : القاعدة الجنائية، دراسة تحليلية لها على ضوء الفقه الجنائى المعاصر، دار النهضة العربية، القاهرة، بدون سنة نشر.
- د. غنام محمد غنام :
- الحماية الجنائية للادخار فى شركات المساهمة، دار النهضة العربية، القاهرة، 1988.
- دور قانون العقوبات فى مكافحة جرائم الكمبيوتر والانترنت وجرائم الاحتيال المنظم باستعمال شبكة الانترنت، دار الفكر والقانون، المنصورة، مصر، 2010.
- د. محمود عبد العزيز محمد السيد الشريف : مدى ملائمة الجزاءات الجنائية الاقتصادية فى ظل السياسة الجنائية المعاصرة، النظرية العامة للجزاء الجنائى الاقتصادى، دراسة تحليلية تأصيلية مقارنة، دار النهضة العربية، القاهرة، 2006-2007.
- د. محمود كيش : المسئولية الجنائية لمراقب الحسابات فى شركات المساهمة، دراسات مقارنة فى القانونين المصرى والفرنسى، دار النهضة العربية، القاهرة، 1992.

- د. محمود محمود مصطفى : الجرائم الاقتصادية في القانون المقارن، الجزء الأول، الأحكام العامة والإجراءات الجنائية، الطبعة الثانية، القاهرة، 1979.
- د. محمود نجيب حسنى :
- علاقة السببية، دار النهضة العربية، القاهرة، 1984
- النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1988.
- جرائم الامتناع والمسئولية الجنائية عن الامتناع، دار النهضة العربية، القاهرة، 1986.
- دروس في القانون الجنائي الدولي، دار النهضة العربية، القاهرة، 1959-1960.
- د. مزهر جعفر عبد السلام : جريمة الامتناع، الطبعة الأولى، الإصدار الأول، دار الثقافة للنشر والتوزيع، عمان، الأردن، 1999.
- د. مصطفى كامل كيره : الجرائم الاقتصادية، دار النهضة العربية، 1983.
- د. مصطفى منير : جرائم إساءة استعمال السلطة الاقتصادية، الهيئة المصرية العامة للكتاب، 1992.

(ج) رسائل الدكتوراه :

- د. عبد الرؤوف مهدي : المسئولية الجنائية عن الجرائم الاقتصادية، في القانون المقارن، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1974.
- د. عبد المنعم محمد إبراهيم رضوان : موضع الضرر في البنيان القانوني للجريمة، دراسة تحليلية تأصيلية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1994.
- د. نائله عادل محمد فريد قورة : جرائم الحاسب الاقتصادية، دراسة نظرية تطبيقية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2013.

(د) أبحاث ومؤتمرات :

- خبير/ عبد الناصر محمد محمود فرغلي ، د. محمد عبید سيف سعيد المسماري : الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2-14/11/1428هـ - الموافق 12-14/11/2007م.

ثانياً : المرجع الأجنبية :

- A. Vitu : La protection pénal de l'interet public et l'interet des associes dans les sociétés commerciales et civiles " Rapport presente aux cinquième journées juridiques Franco-italienne, Paris , Nancy , 5 – 10 juin 1967.
- A. Wiener, theory of economic criminal law Hungarian national group of international association of penal law Budapest 1984 London 1986.
- Maris Cremona, Jonathan Herring MA, Criminal law, Macmilan, 1998.
- Merle et vitu : trait de droit criminel , quatrième édition , 1981.
- Merle- Vitu : Procedure Pénal, 1984.
- Rotman " L'evolutuion de la pense juridique sur le but de la sanction penale Melange Ancel , 1975.
- Stefani, Levasseur, Boulloc : Procedure Penal, 1984.
- U.S. c.Maxwell 45 MJ 406 , 1996; Rene PEPIN, Le statut juridique du cornel au Canada et aux Etats- Unis, www. Lex-electronica. Org/articles/v 2-6/pepin.htm
- United States V. Smith, 27 F. Supp. 2d 111, 16-1115 (C.D. III. 1998).
www.cybercrime.gov/smanual2002.htm

الفهرس

الموضوع	الصفحة
مقدمة	7
الفصل الأول: التعريف بجرائم الاعتداء على الأمن الإلكتروني	9
المبحث الأول : مفهوم الأمن الإلكتروني ومصادر الحماية الجنائية	10
أولاً: مفهوم الأمن الإلكتروني	10
ثانياً: مصادر حماية الأمن الإلكتروني	10
ثالثاً: مفهوم جرائم الاعتداء على الأمن الإلكتروني	12
رابعاً: التمييز بين جرائم الاعتداء على الأمن الإلكتروني وما يتشابه معها	12
خامساً: خصائص جرائم الاعتداء على الأمن الإلكتروني	13
المبحث الثاني: تحديد المصالح محل الحماية الجنائية	16
أولاً: العناصر محل الحماية الجنائية في مجال الأمن الإلكتروني	16
ثانياً: منهج المشرع الإماراتي في تقرير الحماية الفعالة للأمن الإلكتروني	18
الفصل الثاني : الحماية الجنائية الموضوعية للأمن الإلكتروني	21
المبحث الأول : الأركان العامة لجرائم الاعتداء على الأمن الإلكتروني	22
المطلب الأول : الركن المادي في جرائم الاعتداء على الأمن الإلكتروني	23
المطلب الثاني : طبيعة الركن المعنوي في جرائم الاعتداء على الأمن الإلكتروني	37
المبحث الثاني : الجزاءات الجنائية لجرائم الاعتداء على الأمن الإلكتروني	47
المطلب الأول : منهج اختيار الجزاءات المقررة لجرائم الاعتداء على الأمن الإلكتروني	48

55-----	المطلب الثاني : تقييم خطة المشرع الإماراتي في تقرير الجزاءات
61-----	الفصل الثالث: الحماية الجنائية الإجرائية للأمن الإلكتروني
	المبحث الأول : ذاتية قواعد التحري والاستدلال بشأن الاعتداء على الأمن
62-----	الإلكتروني
	المبحث الثاني : ذاتية إجراءات التحقيق الابتدائي بشأن الاعتداء على الأمن
68-----	الإلكتروني
76-----	المبحث الثالث: ذاتية إجراءات المحاكمة بشأن الاعتداء على الأمن الإلكتروني
85-----	الخاتمة
89-----	المراجع
95-----	الفهرس



9 789777 470438

dar.elfker@hotmail.com